

**DETERMINANTS OF FEAR OF CYBERCRIME VICTIMISATION: A STUDY OF
CREDIT/DEBIT CARD FRAUD AMONG STUDENTS OF THE UNIVERSITY OF
SASKATCHEWAN**

A thesis

Submitted to the College of Graduate Studies and Research

in Partial Fulfilment of the Requirements for the Degree of

Master of Arts

in the

Department of Sociology

By

Mohammed A. Abdulai

© Copyright Mohammed Abdulai, May 2016. All rights reserved.

PERMISSION TO USE

In presenting this thesis in partial fulfilment of the requirements for a graduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other use of material in this thesis in whole or part should be addressed to:

Head of the Department of Sociology

University of Saskatchewan

1019- 9 Campus Drive

Saskatoon, Saskatchewan, S7N 5A5

ABSTRACT

Fear of crime studies is an enduring theme in criminological research. The focus of such research, however, has been on conventional physical or place-based crimes. This study was aimed at investigating the fear of Cybercrime (credit/debit card fraud) victimisation among University of Saskatchewan students. This was achieved by asking questions about: 1. students' knowledge/perceptions of cybercrime; 2. exploring their experiences of victimisation; 3. examining students' internet use patterns and frequency; 4. behavioural responses and finally; 5. demography. The study was informed by the framework of Beck's theory of a Risk Society. Beck's view is that given the various unintended consequences of the numerous techno-scientific innovations, risks and hazards have become a permanent feature of the modern time (Beck, 1992). Data was obtained from an online survey of students. Binary Logistic Regression and Cross tabulation were used to predict both fear and risk of cybercrime victimisation.

The findings of the study indicate that prior experience of victimisation and internet use behaviours are both positively associated with students' fear and their risk of becoming victims of credit/debit card fraud. On the other hand, socio-demographic factors and knowledge of cybercrime were both found to be non-significant predictors of students fear and risk of becoming victims of credit/debit card fraud. Based on the findings, the study argues for the need to rethink risks and to further examine reflexivity, as people negotiate the challenge of remaining in the threshold of risk and actual victimisation. The findings from the study demonstrate that the risk society theory has explanatory power and greatly enhanced our understanding of risk in the contemporary technology driven era. The study concludes with a number of recommendations for further studies.

ACKNOWLEDGEMENTS

This humble piece is first and foremost dedicated to the Almighty God in acknowledgement of His presence in all of creation and for His endless bliss and the innumerable countenance He has showered on me right from my time of birth.

Next I register my profound gratitude to my supervisor, Dr. Hongming Cheng for his guidance and supportive role throughout this work. I am highly appreciative for the support.

Again I also want to acknowledge Dr. John Hansen and Dr. Elizabeth Quinlan, as a member of my advisory committee and chairperson for my final defence respectively. Your various inputs and consistent support have been invaluable.

Additionally, I also want to acknowledge the invaluable perspectives and constructive criticisms of my external examiner, Dr. Enchuan Shao from the department of economics.

Moreover, I also want to acknowledge the Forensic Behavioural Science and Justice Studies Centre, for their generous financial support in the form of scholarship with service.

I am also grateful to the Sociology department, in particular the staff of the general office, for the diverse and constant administrative support. Barb, Lori and Kristen, thank you for your patience and constant care.

Finally, I want to acknowledge and thank my family for their eternal support; for their collective efforts have been the kingpin and the prop to my education.

TABLE OF CONTENTS

PERMISSION TO USE	i
ABSTRACT	ii
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
Chapter 1: INTRODUCTION	
1.0. Background	1
1.1. Research Problem	4
1.2. Research Questions	6
1.3. Hypotheses	7
1.4 Contribution/Significance of the study	7
1.5. Definition of terms/Operational definitions	8
1.6. Organisation of the thesis	8
Chapter 2: LITERATURE REVIEW	
2.0. Introduction	11
2.1. Crime Victimisations – White-collar/Corporate and Cybercrimes	12
2.2. The Debates	15
2.2.1. Defining Cybercrimes	15
2.2.2. Dissecting the Criminological Quandary	17
2.2.3. Relationship between Technology and Cybercrime	18
2.3. Characterising Cybercrimes	19
2.4. Types of Cyber fraud and Cybercrime	20
2.5. Terminological Differences	22
2.6. Prevalence of Cybercrime (Credit/Debit card fraud)	23

2.7. Fear of Crime	24
2.7.1. Debates on and Correlates of Fear of Crime	25
2.7.2. Gender and Fear of Crime	25
2.7.3. Income and Race/Ethnicity	29
2.7.4. Marital Status and Education	32
2.7.5. Vulnerability	34
2.7.6. Experience of Victimisation	35
2.8. Measuring Fear of Crime	36
2.9. Chapter Summary	38
Chapter 3: THEORETICAL FRAMEWORK	
3.1. Overview/Introduction	40
3.2. Explaining Fear of Crime (Socio-Criminological Theories)	41
3.2.1. Vulnerability thesis	42
3.2.2. Instrumental thesis	44
3.2.3. Incivilities thesis	46
3.2.4. Psychological factors	48
3.3. Theory of a Risk Society (Beck, 1992)	49
3.3.1. Criticism of Beck's Risk Society theory	53
3.4. Some Contemporary Sociologists on Risks	54
3.4.1. Luhmann: Distinction between Risk and Danger	54
3.4.2. Giddens on Risk	56
3.5. Reflections from the Risk Society Framework	58
3.6. Chapter Summary	60
Chapter 4: METHODOLOGY	
4.1. Introduction	62

4.2. Research Design	62
4.3. Justification for choice of Students	63
4.4. Tools/Survey Instrument	64
4.5. Ethical Considerations	64
4.6. Reflectivity	66
4.7. Hypotheses	67
4.8. Variables	69
4.8.1. Dependent Variables	70
4.8.2. Independent Variables	71
4.8.3. Recoded Variables	72
4.9. Sampling	75
4.10. Analytical Models	76
4.10.1. Generalised Linear Models (GLM)	77
4.10.2. Model Formulation	78
4.10.3. The Link Function	79
4.11. Chapter Summary	79
Chapter 5: FINDINGS	
5.0. Introduction	81
5.1. Descriptives	81
5.1.0. Socio-demographic factors and fear of credit/debit card fraud	81
5.1.2. Full time/Part time study and fear of credit/debit card fraud	82
5.1.3. Residency Status and fear of credit/debit card fraud	83
5.1.4. Place of Residence and fear of credit/debit card fraud	84
5.1.5. Employment/work status and fear of credit/debit card fraud	86
5.1.6. Age and fear of credit/debit card fraud	87

5.1.7. Level of Studies and fear of credit/debit card fraud	88
5.1.8. Ethnicity and fear of credit/debit card fraud	88
5.1.9. Marital Status and fear of credit/debit card fraud	89
5.1.10. Income and fear of credit/debit card fraud	90
5.2. Frequency of Knowledge of Cybercrime	91
5.3. Frequency of Internet use behaviours	92
5.4. Hypothesis Testing	94
5.4.1. Hypotheses 1, 2 and 4	94
5.4.1.1. Results for Hypotheses 1, 2 and 4: Logistic Regression	95
5.4.1.2. Predictions from hypotheses 1, 2 and 4	97
5.4.2. Hypotheses testing: Hypothesis 3	99
5.4.2.1. Results for hypotheses 3: Logistic Regression	99
5.4.2.2. Predictions from hypotheses testing: Hypothesis 3	107
5.5. Chapter Summary	107
Chapter 6: ANALYSIS AND DISCUSSION	
6.0. Introduction	109
6.1. Impact of knowledge of cybercrime on fear of credit/debit card fraud	109
6.2. Impact of Socio-demographic factors on fear of credit/debit card fraud	111
6.3. Impact of Internet use behaviours on risk of credit/debit card fraud	114
6.4. Impact of Past experience of victimisation on fear of credit/debit card fraud	118
6.5. Chapter Summary	120
Chapter 7: CONCLUSION	123
7.1. Theoretical and Policy Implications	125
7.2. Limitations and Agenda for future research	128

BIBIOGRAPHY	131
APPENDIX: The Survey Questionnaire	141

LIST OF TABLES

Table 5.06: Chi-Square Test and Descriptive Statistics for relationship Between Age and Fear of Credit/Debit card fraud victimisation	87
Table 5.07: Chi-Square Test and Descriptive Statistics for relationship between Level of studies and Fear of Credit/Debit card fraud Victimisation	88
Table 5.08: Chi-Square Test and Descriptive Statistics for relationship between Ethnicity and Fear of Credit/Debit card fraud victimisation	89
Table 5.09: Chi-Square Test and Descriptive Statistics for relationship between Marital status and Fear of Credit/Debit card fraud victimisation	90
Table 5.10: Chi-Square Test and Descriptive Statistics for relationship between Ethnicity and Fear of Credit/Debit card fraud victimisation	91
Table 5.11: Frequency distribution of respondents Knowledge of Cybercrime	91
Table 5.12: Frequency distribution of Medium of Internet access by respondents	92
Table 5.13: Frequency distribution of number of times of Online Purchases by Respondents	92
Table 5.14: Frequency distribution of Online Safety precautions adopted by Respondents	93
Table 5.15: During the past month, have you ever felt fearful about being the Victim of credit/debit card fraud?	95
Table 5.16: Compared to other crimes (physical crimes), do you feel more At risk of Credit/Debit Card fraud?	99
Table 5.17: Cross tabulation of the relationship between medium of internet access and risk of Credit/Debit card fraud victimisation	103
Table 5.18: Cross tabulation of the relationship between number of times of	105

Online purchase access and risk of Credit/Debit card fraud

Victimisation

Tale 5.19: Cross tabulation of the relationship between Online safety precautions 106

And risk of Credit/Debit card fraud victimisation

LIST OF FIGURES

5.01: Relationship between Gender and Fear of Credit/Debit card fraud	81
5.02: Relationship between Study mode and Fear of Credit/Debit card fraud	83
5.03: Relationship between Study mode and Fear of Credit/Debit card fraud	84
5.04: Relationship between Place of residence and Fear of Credit/Debit card fraud	85
5.05: Relationship between Current employment/work status and students' Fear of Credit/ Debit card fraud	86

CHAPTER 1

INTRODUCTION

1.0. Background

In recent times, fear of crime research has come to the fore of criminological and forensic research due to its significance in contributing to an understanding of the predictors of crime, as well as coming up with policy interventions. Research into fear of crime meanwhile is mostly focused on conventional or physical place-based crimes, however, cyberspace has increasingly changed the nature and scope of criminality (offending and victimization) (Jaishankar, 2008). Cross country data has revealed that cybercrimes, specifically credit/debit card fraud has seen a drastic increase, with a rising concern and fear of victimisation in the USA, Australia and Britain (Fox, 2001; Australian Bureau of Statistics, 2008; Roberts, Indermaur & Spiranovic, 2013).

Within the Canadian context, cybercrimes are equally prevalent and have raised significant concerns. Specifically, identity theft is reported to be the fastest growing type of fraud in North America by the Canadian Council of Better Business Bureaus, with losses in the billions of dollars each year (Smyth, 2010). Against this backdrop, more than 12, 000 cases of identity-theft complaints were reported in Canada by PhoneBusters, with losses amounting to over \$9 million (Smyth, 2010: 45). From all indications, this is likely to continue growing into the foreseeable future, especially as more transactions are performed online, and as internet usage increases (Arango, Huynh, Fung, & Stuber, 2012).

The growth in the volume and value of online transactions over the past two decades warrants concerns over the risks of cyber fraud. According to StatsCan (2009), in 2001 there were 13.4 million online orders made by over 2.2 million households. By 2007, this

figure had grown to nearly 70 million orders by about 8.4 million Canadian individuals aged 16 years and older. This growth creates previously unimaginable opportunities for cyber frauds, including stealing identities and hacking customers credit/debit card details from retailers or from their personal devices. In fact, Grau (2008) notes that concern over the security of credit card payments holds Canadians back from buying more online.

Concerns about cybercrimes are not only a personal issue, but it often concerns both the business community as well as government. Businesses have been forced to incur huge costs to upgrade their ICT security as well as to insure against cybercrimes. For example, it is estimated worldwide that organisations spent more than \$71billion in 2014 on information security, which is expected to grow by over 8% in 2015 and way into the foreseeable future (CloudMask, 2016). In fact, these concerns have already impelled national agencies and the Canadian government to come up with strategies aimed at curtailing the menace. In Canada, for example, coming up with a “whole-of-government approach to cybersecurity” was identified as a strategic priority by the Public Safety and Emergency Preparedness Canada in its 2009-10 report (Ministry of Public Safety, 2009:10). Then again, another practical response to the problem of cybercrime in Canada was the launch of the PhoneBusters initiative by the Ontario Provincial Police to counter telemarketing fraud (Smyth, 2010:55). PhoneBusters is the Canadian central agency for the collection of information about telemarketing, fraud and identity theft (Smyth, 2010).

At the global stage, efforts have been made to counter the problem of cybercrime. The Council of Europe *Convention on Cybercrime* called the *Convention*, was the first international treaty on crimes committed on the internet (Council of Europe, 2001). The treaty, to which Canada, the USA and Australia among other nations are signatories, provides a framework for international co-operation, aimed at pursuing common criminal policies. The treaty though represents a significant step at bridging the problem of jurisdiction, require

an almost universal ratification and implementation by countries the world over to ensure the realisation of the full benefits of the initiative.

Notwithstanding these practical steps, however, combating cybercrime still remains a challenge for law enforcement and criminal justice in Canada (Smyth, 2010). Some of the challenges identified by Smyth (2010) include the problem of under-reporting by both individuals and corporations; the small impact nature of cybercrimes and the fact they fall outside routine police duties; as well as the lack of expertise, in the sense that the technical knowledge and expertise to deal with cybercrimes are absent from the training of most police officers. Other challenges involve the problem with boundary or jurisdiction – geographical distance between victim and offender (Smyth 2010:18, 54-55). However, these challenges are not unique to the Canadian context; instead, they are intrinsic to the problem of cybercrime within the wider global context. For example, the problems of definition and boundary have been acknowledged in the literature (Jaishankar, 2008; Valiquet, 2011).

The internet has therefore opened up new avenues for criminal behaviours, including how fears are experienced among (potential) victims, and the way crime in general is researched. Consequently, this project attempts to contribute to the scholarship on cybercrime through an empirical analysis of how university students experience cybercrime fear/victimisation, and the determinants of such fears. It is dedicated to the study of credit/debit card fraud victimisation among students at the University of Saskatchewan. The thesis will specifically examine the determinants of fear of credit/debit card fraud (that is, a specific cybercrime) among students. Data collected through an online survey will be used to understand the predictors of fear of credit/debit card fraud victimisation from the perspective of students as reflexive agents. The data will be analysed within the framework of themes arrived from a review of the literature. This thesis is situated within the framework of Beck's risk theory and as such, the analysis will be guided by the tenets of Beck's theory.

1.1. Research Problem

Fear of crime research is an enduring focus among criminological researchers (Hale, 1996). The enduring interest has led researchers into exploring various themes of interest. Some of the themes identified in the literature include perceptions and predictors of fear of crime, possible consequences of fear, factors contributing to the fear of crime and the role of the situational environment as a crucial element in the formation of perceptions of individual security (Bannister, 1993; Box, Hale & Andrews, 1988; Wilson, 1975 and Taylor & Hale, 1986). The field has, as well, generated much controversy in relation to contrasting findings by researchers. Some of the contentious issues involve the precise meaning and reality of 'fear of crime'; the role of the media in affecting fear of crime; the impact of gender on fear of crime; and the impact of community on fear of crime among others.

The literature acknowledges that criminological research has had an overarching emphasis on “‘ordinary’ street crime rather than corporate or white collar crime” and consequently research into fear of crime has followed a similar path (Hale, 1996:84). Additionally, researchers rely on “a global measure (so called because the question makes no reference to a specific crime)” to measure fear of crime (Hale, 1996:85). On the contrary credit/debit card fraud – a typical cybercrime – has seen a drastic increase over the years across countries without corresponding academic attention. Nonetheless, there is increasing global interest in cybercrimes. For example, the Pew Internet and American Life project report show that majority of Americans (that is 87%) revealed concerns about online credit card theft, with another majority (69%) reporting being ‘very concerned’ (Fox, 2001). Similarly, population estimates from a fraud survey in Australia revealed that whereas 3.1% of Australians over the age of 15 years were victims of identity fraud, majority of the respondents (77%) were victims of bank card or credit card fraud (ABS, 2008). In addition, the British Crime Survey of 2005/06 revealed that more than half (57%) of respondents

owning credit cards reported being ‘fairly’ or ‘very worried’ about being a victim of card fraud (Roberts, Indermaur & Spiranovic, 2013:10). Specifically in Canada, PhoneBusters – the Canadian central agency for collecting telemarketing, fraud and identity theft information – reported instances of 12, 142 cases of identity-theft complaints in Canada, with losses amounting to \$9,590,385 (Smyth, 2010: 45).

Apart from the direct costs of cybercrimes (credit/debit card fraud) as identified in the literature (Smyth, 2010; StasCan, 2009), there is also an indirect cost to the prevalence and perpetuation of credit/debit card fraud (Smyth, 2010; Anderson, Barton, Böhme, Clayton, Van Eeten, Levi, Moore and Savage, 2013). “Indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime” (Anderson et al., 2013:271). Examples of these costs include the loss of trust in online banking and its consequent impact on reduced revenues from electronic transaction fees (Anderson et al., 2013; Smyth, 2010). The loss of trust in online banking can have even far reaching consequences, for example as Grau (2008) identified, concern over the security of credit card payments holds Canadians back from buying more online. Another aspect of indirect cost could be seen from the costs to businesses and institutions incurred in their resolve at protecting the cyber landscape. These costs have been captured differently in other literature as defence costs and include spam filters, antivirus and browser extensions among others (Anderson et al., 2013). Though seen as indirect, the real value of the losses from indirect costs is substantive. For example, “the botnet behind a third of the spam sent in 2010 earned its owners around \$2.7 million while worldwide expenditures on spam prevention probably exceeded billion dollars” (Anderson et al., 2013:266).

Imperatively, the above researches and evidence suggest that cybercrimes must receive increasing academic scrutiny, if they are to be properly understood and if effective

interventions are to be developed. Furthermore, technological advancements of the 21st century are increasingly making cybercrimes unintended consequences, which makes it imperative that fear of crime research begin to focus on cybercrimes as well. My research problem therefore arises from this observation. The specific problem is what explains the fear of credit/debit card fraud victimisation among students? This question will be answered using the framework of Beck's Risk theory. The crux of the Risk Society theory is that given the various unintended consequences of the numerous techno-scientific innovations, risk and hazards have become a permanent feature of the modern time (Beck, 1992).

Approaches like the one adopted in this thesis would help in arriving at a much nuanced understanding of the victimisation as well as fear of various forms of crimes and specifically credit/debit card fraud. This research is therefore intended to contribute towards filling the void in criminological literature, no matter how small a contribution it may be.

1.2. Research questions

This study seeks to understand the determinants of fear of credit/debit card fraud victimisation among university students at the University of Saskatchewan. In order to do this, it asks the following four questions:

1. How do students' perception /knowledge of cybercrime impact how fearful they are of becoming victims of credit/debit card fraud?
2. In what ways do socio-demographic factors affect fear of credit/debit card fraud victimisation among university students?
3. Do students' internet use behaviours make them vulnerable to risk of credit/debit card fraud victimisation?
4. How does past experience of credit/debit card fraud victimisation affect fear of future credit/debit card fraud victimisation among university students?

These questions are significant because even with broad based ‘ordinary’ street crime, questions relating to the significance of factors, for example socio-demographic factors and previous experience of victimisation on fear of crimes, yield inconclusive results. The gendered argument under socio-demographic factors, for example readily stands out among other unsettled findings. It is therefore important that we can produce as much disaggregated information as possible on cybercrimes, because it might have implications for ‘ordinary’ crimes. Furthermore, the answers to the above research questions therefore have implications for our understanding of Beck’s theory of risk society.

1.3. Hypotheses

To understand the problem and to arrive at answers to the research questions, this thesis will test four hypotheses in line with the research questions. The hypotheses to be tested include:

1. Students who believe cybercrime is both cyber-enabled and cyber-dependent are less fearful than students who believe cybercrime is either cyber-enabled or cyber-dependent.
2. Socio-demographic factors significantly affect fear of credit/debit card fraud victimisation (females, older people, single, non-whites with higher income are expected to be more fearful of credit/debit card fraud victimisation).
3. Internet use behaviours increases students’ risk of credit/debit card fraud victimisation.
4. Past victims of credit/debit card fraud are more fearful of credit/debit card fraud victimisation.

1.4. Contribution/Significance of the Study

By applying what is known about fear of crimes in general to cybercrime (credit/debit card fraud) specifically, this research will allow us to identify linkages (if any) between the

two, and suggest how the growing threat of cybercrimes can be addressed proactively. It also represents a significant step forward in understanding risk factors and cybercrime victimisation. As the literature shows, with increasing internet use behaviour, cybercrimes are expected to explode. By identifying risk factors, preventative measures can be proposed to eliminate the risks in advance of an explosion of these types of crimes. The study is also significant in that it addresses a potential future problem, which is an advance in how researchers approach problems. Rather than being reactionary, the results can suggest proactive measures to addressing fear and risk factors of cybercrimes. The study also makes a theoretical contribution to the field of fear of crime research by providing much disaggregated information on a contemporary problem, which transcends boundaries, and on the upward surge.

1.5. Definition of terms/Operational Definitions

1. Credit/Debit card Fraud – is the same as credit/debit card theft and will be used interchangeably
2. Place-based, Physical crime and Conventional crime – all refer to the same phenomenon and are used interchangeably in this work.
3. Cybercrime, Cyber-crime – both refer to the same phenomenon in the context of this study.

1.6. Organization of the thesis

The rest of the thesis is organised around six chapters.

Chapter 2 begins with a review of general themes in white-collar and corporate crime victimisation, with a view to providing conceptual and theoretical clarity. This is deemed necessary before getting into the main thrust of the thesis. Next, the chapter presents a review of the literature on key debates in cybercrime such as the definition, the criminological quandary, relationship between technology and cybercrime. It also discusses the prevalence

of credit/debit card fraud, drawing on empirical research from around the globe. A major part of the literature here also includes fear of crime, correlates of fear of crime and finally measurement of fear of crime. This allows me to identify the issues that are relevant to my study and to be able to define my contribution to the field.

Chapter 3 provides a theoretical literature review on the issue of cybercrimes and justifies the theoretical framework adopted for the thesis. Socio-criminological theories reviewed include vulnerability thesis, instrumental thesis, incivilities and psychological factors. Beck's theory of Risk society, which is the theory guiding the study is thoroughly reviewed, with specific emphasis on why it is relevant to this research. The works of contemporary sociologists on risk is also reviewed in the chapter. The sociologists include Luhmann and Giddens. The chapter concludes with a general reflection from the risk society framework.

Chapter 4 addresses the methodological issues and research design used in the research. Justification is provided for the choice of population and sample. Variables for the study (dependent and independent) are identified with a further provision of the variables that were recoded with an explanation of the rationale in each case. It is then followed by a description of the sampling framework and the statistical model, with a description of both the model formulation and link function.

Chapter 5 presents the results of the study. The findings are presented thematically, in accordance with the hypothesis and research questions. The study found that victimisation experience and internet use behaviours are both positively associated with students' fear and their risk of becoming victims of credit/debit card fraud. Specifically, past victims expressed more fear than students without prior experience of victimisation. Also all the internet use variables but one, were significantly related to increased risk of victimisation. On the other hand, knowledge of cybercrime and socio-demographic variables were found to be non-

significant and hence, made no significant difference to students' fear and risk of becoming victims of credit/debit card fraud. These findings confirm that the theory of Risk society has explanatory power. Beck's theory of risk espouses that risk is system immanent and inescapable, which means that it affects everyone regardless of socio-demographic status such as gender and marital status. This explains why these were found to make no significant difference on fear of credit/debit card fraud.

Chapter 6 builds on the previous chapter through analyses and discussions of the findings in light of the research questions. These include knowledge, socio-demographic variables, internet use behaviours and victimisation experience.

Chapter 7 presents a summary or conclusion of the study and especially of the findings. Some theoretical and policy implications of the findings are examined and conclude with a discussion of the limitation and agenda for future research.

CHAPTER 2

LITERATURE REVIEW

2.0. Introduction

The fields of fear of crime and cybercriminal studies and research have generated significant controversies, with few, if any points of agreement between scholars in criminological studies and forensics. The scholarly disagreements result from contrasting findings in relation to key thematic areas of study. The lack of a unified, consistent and statutory definition of cybercrime has been acknowledged by scholars and institutions (Canadian Centre for Justice Statistics & Kowalski, 2002; Smith, Grabosky & Urbas, 2004; Smyth, 2010, Valiquet, 2011; and Yar, 2005). As well as this, defining and measuring fear have also courted significant controversy. In the midst of these controversies, however, the continuous significance and severity of fear of crime remain unchallenged.

Related to the definitional and measurement problems are concerns about the impacts of the media and community in fostering fear. Most significantly especially for the present study, are questions of the determinants of fear of crime, and specifically of cybercrime (credit/debit card fraud victimisation). Is fear gendered? Is fear affected by age as well as victimisation experience? These are among several crucially important and yet controversial dimensions to understanding the menace of fear of crime (cybercrime). These questions represent just a few of the dimensions but yet not much consensus has been established in relation to them.

The rest of the review in this chapter will proceed in the following order: section 2.1 reviews literature on the general themes in white-collar/corporate crime and cybercrime victimisation. The idea in this section is to provide conceptual and theoretical clarity before

moving on to the substantive themes of the thesis. The next section (2.2) focuses on a review of the key debates in the study of cybercrime and victimology. Debates reviewed include defining cybercrime, the criminological quandary, the relationship between technology and cybercrime and characterising cybercrime. Other debates include the types of cybercrime, terminological differences and prevalence of cybercrime. The rest of the chapter looks at prevalence of cybercrime (credit/debit card fraud), fear of crime, correlates of fear of crime and measuring fear of crime. These debates are very important because understanding them contribute to a great understanding of the subsequent discussion in the thesis.

2.1. Crime Victimisations – White-collar/ Corporate crimes and Cybercrimes

Criminal victimisation has thrown up interesting and at times difficult observations. Some of the challenge arising from studies into criminology and victimology has centred partly on the distinctions between white-collar and corporate crime on the one hand and cybercrimes on the other hand. To ensure some conceptual and theoretical clarity, this section will provide an exploration into general themes in white-collar and corporate crime victimisation, before delving into the main thrust for the present study, that is, cybercrime (credit/debit card fraud) victimisation.

As Hale (1996) argued, white-collar and corporate crime is an area that has not received much attention like physical place-based crimes. The resort to conventional conceptions of crime has meant white-collar crime is not the focus of mainstream criminology and victimology (Croall, 2001b:36). This neglect, however, is problematic as it has the potential of leaving out an important realm of criminality, and hence its potential victims. And unlike physical crimes, consumers constitute a major target group for white-collar and corporate crime victimisation, even though many of the activities affecting them are not classified as crime (Croall, 2009). As a result, consumers have been considered a

relatively undifferentiated group, all of whom are open to being victimised. This also partly accounts for the lack of much research interests in the area.

However it has been strongly argued that while all consumers are at risk, the impact of consumer and white-collar crime like other forms of crime, reflect wider patterns of structural inequality and falls most severely on the most disadvantaged – vulnerable groups (Croall, 2001b; 2009:127). Vulnerability as used here is in reference to traditional sociological variables such as age, gender and socio-economic status (Croall, 2001b). Thus the structural variables account for differences in white-collar crime victimisation. It has also been argued that white-collar crime victimisation reflects the difference between two options – a theoretical possibility and a practical occurrence (Shapiro, 1990). That is to say, even though it is believed that almost everyone is at risk of white-collar crime victimisation, in reality only a section of the population – defined predominantly by their social structural location - actually get victimised. Employers for example, utilise risk avoidance, which is not available to non-employers and people lacking the resources or expertise, to protect themselves from certain victimisations (Shapiro, 1990).

The defining features of white-collar crime victimisation (from the ‘conventional’ conception) include that it is relatively invisible, indirect and impersonal (Croall, 2001b). However a critical approach reveal victimisation is much broader and involves physical and economic harms, along with threats to the quality of life and community safety (Croall, 2001b). On the basis of this, the critical approach has been suggested as the preferred option with a view to arriving at a comprehensive understanding of white-collar crime victimisation. Critical victimology as advocated examines victims and crimes considered hidden in the conventional sense, as well as the structural and individual dimensions of victimisation (Mawby & Walklate, 1994).

Significantly for Slapper and Tombs (1999), the study of white-collar crime victimisation is an under-researched area within the realm of 'white-collar criminology', with not much interest from scholars. The limited research observation, however, appear to result partly from the fact white-collar crime is seen as non-conventional crime. Importantly, the lack of interest could also be due to the fact white-collar crime disproportionately affect people in the lower ranks of the class structure, as Croall (2001b, 2009) suggested earlier. Additionally, white-collar crime victimisation is neglected from studies for two main reasons - technical and ideological (Croall, 2001b:37). Technical reasons include "methodological difficulties of researching white-collar crime victimisation" - invisibility and indirect victimisation makes it difficult to arrive at estimates from official criminal statistics, conventional crime surveys and crime audits (Croall, 2001b:37). Ideologically white-collar crime does not "'fit' conventional notions of crime and victimisation" (Croall, 2001b:37). Consequently for an effective study of white-collar crime victimisation, white-collar criminologists need to follow in the steps of critical victimology and apply a 'white-collar crime lens', with the view of exploring the many dimensions of victimisation (Croall, 2001b:40).

In conclusion to this brief section, it is imperative to mention that both white-collar crimes and cybercrimes differ from mainstream 'conventional' place-based crimes, but are also different in themselves in significant ways. Both types of crimes constitute relatively invisible and indirect criminal activities. However, whereas cybercrime especially credit/debit card fraud is perpetrated using technology, white-collar crimes can be committed without the use of technology. Again white-collar crimes are mostly committed by people of power, office and some influence. Cybercrime on the other hand can be committed basically by anyone with a rudimentary knowledge in the use of computers. Having said these and briefly exploring some general themes in white-collar crime victimisation so far, attention

now moves into the debates on cybercrime victimisation - the main focus of the present study.

2.2. THE DEBATES

2.2.1. Defining Cybercrime

Defining cybercrime remains one of the daunting tasks of policy makers, scholars in criminological theory and several other stakeholders with various levels of interest in the phenomenon. A 2002 Statistics Canada publication explicitly recognises this problem of the lack of a unified definition. The concept lacks a consistent and statutory definition (Parliamentary Joint Committee on the Australian Crime Commission (PJCACC), 2004; Valiquet, 2011; Yar, 2005) and as a result the difficulty in finding an overarching definition. The definitional difficulty is also heightened by the fact that defining cybercrime raises conceptual complexities (Smith, Grabosky & Urbas, 2004). Perhaps the conceptual complexity of cybercrime reflects its dynamic nature, while concepts to describe it so far remain static and sensitive to either space, time or both. Cracking the conceptual difficulty then, require coming up with equally dynamic concepts that are flexible, and as well have a consistent application across time and space.

The Oxford online dictionary defines cybercrime as “criminal activities carried out by means of computers or the internet” (Oxford Dictionaries, 2014). The yardstick from this definition is either “computers” or “the internet” and consequently carries with it a much broader perspective. However, a careful observation reveals the definition caters only for the ‘where’ or place but silent on the ‘how’ which is nonetheless, a very crucial consideration in efforts at better understanding cybercrime. Also in their study dubbed “*Seeing Beyond the Surface ...*” Longe, Mbarika, Kourouma, Wada and Isabalija define cybercrime as

misconducts in the cyberspace as well as wrongful use of the internet for criminal purposes” (Longe et al., 2009:124).

On his part, Jaishankar (2008) makes reference to two categories of cybercrime as identified at a workshop during the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, “thus: (a) Cyber crime in a narrow sense: any illegal behaviour directed by means of electronic operations that targets the security of computers systems and the data processed by them; (b) Cyber crime in a broader sense: any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or disturbing information by means of a computer system or network” (Jaishankar, 2008:286). The UN Congress’ perspective and especially its second category is significant, as it attempts to cater for all the possible dimensions of cybercrime. However, this perspective comes short when one take into consideration variations of cyber criminality where offenders lure unsuspecting victims via the phone, without having to resort to any computer system throughout the process. Inevitably and in relation to this, it comes down to the definition of a computer system.

Another frequently reported and utilised definition of cybercrime is the one provided by the Canadian Police College. It defines cybercrimes as crimes where a computer is used as the tool and object of the crime (Canadian Centre for Justice Statistics & Kowalski, 2002). The Canadian Police College definition obviously gives rise to two and possibly three main types of cybercrime, thus one where the computer is used as the tool, another where a computer is the object of the crime and a third variation where the computer is simultaneously the tool and object of the crime. By virtue of the breath of the definition, therefore most other definitions are likely to be subsumed under it as you will find, they either mention the computer as the tool or the object, one way or the other.

For the purpose of this study, the Canadian Police College's definition of cybercrime will serve as my reference for defining cybercrime.

2.2.2. Dissecting the Criminological Quandary

Smyth (2010) argues for distinction between “old” or conventional crimes, “new” crimes which use technology and quasi-traditional crimes (2010:16). This distinction carries with it the notion of the criminological quandary, which Yar (2005) describes as carrying with it the question whether it is an entirely new crime or an old one but in a different form. Several authors have differed on this theme, perhaps consistent with the general controversies on the subject. Grabosky contend that cybercrime is basically a situation of “new wine in old bottles”, implying “...less a question of something completely different than a recognizable crime committed in a completely different way" (Grabosky, 2001:243). Essentially, ““virtual criminality”” is the same as the ‘terrestrial crime’ with which humans are familiar” (Grabosky, 2001:243). On the other hand Yar (2005) argues cybercrime is the case of “Old wine in bottles of varying and fluid shape”. Meanwhile on the contrary Wall (1999) argues from the position that cybercrime is “New wine in no bottles”.

Two fundamental points arise from the argument over the criminological quandary: first, cybercrime is not an entirely new set of crimes but it is dynamic; second cybercrime is a novelty, an entirely new form of criminal activity but without an indication of the nature it takes. It is therefore evident that one's position on the quandary is a reflection of her/his understanding of the problem. My position is that cybercrime constitute Both New and Old wines, but in new bottles, that is, new and at the same time old crimes with both utilising new and ever changing technological innovations.

2.2.3. Relationship between Technology and Cybercrime

The 21st century especially has variously been touted as the age of technology with numerous breakthroughs and improvements across the different facets of life. Scientists, and most others trusting in the scientific discourse, are of the view that these breakthroughs can only be beneficial for the wider society. For disciplinary fields such as the sociology of science and knowledge where an attempt is made to understand science as a set of social relations (Hird, 2012), this discussion is of immense significance.

In the sociology of science, a major argument surrounds the claim to the purity of science. Essentially, the claim consists in the view that science is an illuminating and a superior subject laden with beneficial consequences for humanity. To this end, this claim can be situated in the above debate. On the theme of cybercrime and technology, however, that overarching sense of optimism and positivity of technology is not quite straight forward. Much of the literature sounds pessimistic and mostly point to technology as rather opening up and enhancing opportunities for criminal behaviour in various dimensions (Beck, 1992; Cox, Johnson & Richards, 2009; UN in McCusker, 2006).

In the view of Cox et al. (2009) “It seems obvious that the opportunity for crime is multiplied by the simple fact the criminal is no longer “place-bound.” The potential victim is far more likely and more frequently to be exposed to an offender, through the internet” (Cox et al., 2009:311). This therefore suggests a situation of pessimism more than optimism.

The United Nations (UN) 1992 observation that societal evolutionary processes, including technological development, have only strengthened criminal and powerful organisations (McCusker, 2006), suggest a lucid recognition of the seemingly inevitable fact. Obviously an institution such as the UN making such an observation only points to the seriousness of the issue.

From the above, the purity of science claim in the discourse of the Sociology of Science and Knowledge can be put into perspective. Processes of technological development can indeed be messy, disordered and without automatically leading to the desired outcomes or while reaching the desired outcomes, it could also leave in its wake serious challenges such as cybercrimes in this context. Therefore the need for a specific study into the fears of such crimes resulting from processes of technological development is only strengthened by the above.

2.3. Characterising Cyber Crimes

Cybercrime just like any activity comes with defining attributes. A significant step on the way to better understanding cybercrime is in getting a grasp at these defining characteristics. As dynamic a concept cybercrime is, the extensive nature of its attributes comes as no surprise.

In an effort to distinguish cybercrimes from physical crimes, Brenner (in Jaishankar, 2008: 290-291) outlines the following significant features of cybercrime;

1. Transnational nature and jurisdictional issues. That is, cybercriminals operate without limits of boundary and can work over multiple sources at a time.
2. Physical constraints – that the physical constraints dictating action in the physical world does not apply to cybercrime.
3. Proximity – cybercriminal activity does not require physical proximity between victim and offender.
4. Scale and multiple victimisations. That cybercrime is an automated crime which can target multiple victims simultaneously with the same level of effort.
5. Conduct at issue may not be illegal. That a key feature of cybercrime is that a particular cybercriminal act might be deemed illegal in one jurisdiction and not in

another. For example the “Love Bug” virus in May 2000 which originated from the Philippines.

6. Perfect anonymity – that people are able to disguise themselves in ways not possible in physical crime.
7. Velocity - this is in reference to the speed at which cybercrimes get perpetrated.

My conceptualisation of cybercrime for this study is one that exhibits the above features as suggested in Jaishankar above. More specifically, credit/debit card fraud as a typical cybercrime is often committed by people from distant locations, with their targets in other locations as well. For example, Durkin and Brinkman’s discussion of 419 fraudsters or credit card fraudsters also known as yahoo boys in Nigeria, reveals that although practised from Nigeria in distant West Africa, their targets are mostly in Europe and North America (Durkin & Brinkman, 2009). It also reveals that the perpetrators have no physical constraints or need proximity in order for them to carry out their criminal acts. Credit/Debit card fraud offenders are also able to simultaneously target multiple victims across different locations and with the same level of effort. Significantly the absence of an all-encompassing international and jurisdiction neutral law on credit/debit card fraud and hence cybercrimes, is relevant for my consideration of credit/debit card fraud. And what is more, credit/debit card fraud is perpetrated by ‘invisible’ people hiding under the anonymous world of cyber interface. From the above therefore, my conceptualisation of credit/debit card fraud as a typical cybercrime, thus exhibits the characteristics of cybercrimes as outlined by Brenner in Jaishankar (2008).

2.4. Types of Cyber fraud and Cybercrime

Immediately related to the defining features of cybercrimes is the types of cybercrime. Consistent with the general line of controversies on the subject, there is little consensus on

the types of cybercrimes, with there been a wide array of types and variations frequently mentioned in the literature.

Yar (2005:410) has described four types of cybercrimes namely;

1. Cyber-trespass – crossing boundaries into other people’s property and/or causing damage, e.g. hacking, defacement, viruses.
2. Cyber-deceptions and thefts – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. ‘piracy’).
3. Cyber-pornography – activities that breach laws on obscenity and decency.
4. Cyber-violence – doing psychological harm to, or inciting physical harm against others , thereby breaching laws pertaining to the protection of the person, e.g. hate speech, stalking.

Jaishankar (2008) also citing the Council of Europe Convention on Cybercrime, makes reference to four main categories of cybercrimes including;

1. Offenses against the confidentiality, integrity, and availability of computer data and systems
2. Computer-related offenses
3. Content-related offenses (e.g., child pornography) and
4. Offenses related to infringements of copyright and related rights.

From the several types mentioned, it is evident that authors generally share similar understandings about the nature of cybercrime, even if they differ in the details. There are instances where somewhat different concepts are used but tending to carry the same implicit understanding. This observation is very consistent in most of the cybercrime literature.

Having said these, however, the above categorisations appear overly broad, expansive and at times confusing. For the purpose of this study therefore, I would rely on the categorisations suggested by McGuire and Dowling (2013). According to them, the internet provides both a new means of committing established crimes and also provides opportunities to undertake new types of crimes. The former is categorised Cyber-enabled and the latter Cyber-dependent (McGuire & Dowling, 2013). Cybercrimes therefore include:

- Cyber enabled offenses e.g. include fraud, theft, sexual offenses; and
- Cyber dependent offenses e.g. include computer hacking, viruses.

2.5. Terminological Differences

There is also controversy on the terminology used to describe cybercrime. It is referred to in several contexts in terms such as computer crime, computer-related crime, digital crime, information technology crime, internet crime, virtual crime, e-crime and net crime (Jaishankar, 2008; Lastowka & Hunter, 2004; Maat, 2009; Mann & Sutton, 1998; Smyth 2010; Wall, 2001). In addition to the above, it is also referred to in parts of Africa as “419” and “Sakawa” (Boateng, Olumide, Isabaliya & Budu, 2011; Longe et al, 2009; McCusker, 2006; Warner, 2011).

Although referred to in different terms, sometimes the reference is to the same cybercriminal activity such as computer-related crime and cyber-trespassing, cyber fraud and e-crime, cyber-pornography and content-related crimes among others. This inconsistent use of terminologies, however, can be problematic as it could lead to generalisation of different offences. For McCusker (2006), the arbitrary use of terms can blur significant distinctions between, for example, cybercrime and organised crime. McCusker therefore concludes that “there remains a confused and confusing plethora of terminology, purported parameters and alleged participants of cybercrime ...” (McCusker, 2006:258).

The controversy generated from terminology could be a result of the initial challenge of establishing a unified conception for the phenomenon. The fact reality is different for people across time and space is a plausible explanation as well. Having said this, it is possible that with a concerted effort by scholars especially in the criminological field, some of these controversies can be done away with. The setting up of well-defined parameters or yardsticks could be the way to go. Policy makers and other interested parties will then be able to feed off this.

2.6. Prevalence of Cybercrime (Credit/Debit Card Fraud)

Criminality has been affected by processes of technological and scientific advancements. Specifically, cyberspace has increasingly changed the nature and scope of criminality (offending and victimization) (Jaishankar, 2008). Meanwhile the need to use the cyberspace for personal, academic, business and other concerns keeps rising by the day. Significantly internet use over the years is increasing, with the Canadian Internet Use Survey reporting that “83% of Canadians aged 16 and over accessed the internet for personal use in 2012. A majority of Internet users in Canada did their banking online (72%), visited social networking sites (67%), and ordered goods and services online (56%). The total dollar value of orders placed online by Canadians reached \$18.9 billion in 2012” (Statistics Canada, in Mazowita & Vézina, 2014). Against this background, the Canadian police (comprising select police services policing 80% of the population), recorded 9,084 incidents of cybercrime in its 2012 report (Mazowita et al., 2014).

Much disaggregated information on the prevalence of specific cybercrimes gives a better context to the problem. Cross-country data reveals an increased incidence of credit/debit card fraud, as a typical cybercrime. The Pew Internet and American Life project report show that majority Americans (87%) revealed concerns about online credit card theft,

with another majority (69%) reportedly being 'very concerned' (Fox, 2001). Population estimates from a fraud survey in Australia revealed that whereas 3.1% of Australians over the age of 15 years were victims of identity fraud, majority of the respondents (77%) were victims of bank card or credit card fraud (Australian Bureau of Statistics, 2008). Also the British Crime Survey of 2005/06 revealed that more than half (57%) of respondents owning credit cards reported being 'fairly' or 'very worried' about being a victim of card fraud (Roberts et al., 2013:10).

On the contrary given that most cybercrime victims do not report to the police for very different reasons (Smyth, 2010); it is apparent the prevalence statistics is an understatement of the reality and severity of cybercrime.

2.7. Fear of Crime

Fear of crime has generated much research interests among criminologists. Researchers have sought to understand the various elements and influences on fear of crime among other themes. An important factor for the increase in the work on fear of crime was the discovery that fear of crime far exceeded crime's objective reality (Hale, 1996). The argument over fear of crime's objective reality therefore, for Hale (1996) has become fundamental to research interests in fear of crime. For example, Warr (2000) poses the question; does fear of crime really reflect a fear? Warr's question is, however, more judgement laden, and would depend to a great extent on the perspective of the person involved. To this extent Whitrod (1982) is of the view that fear of crime is unrelated to actual patterns of victimisation rather, Whitrod argues, it is the result of people's perception of their vulnerability following from the subjective judgement of their personal risk. On the other hand some researchers are concerned about measuring fear of crime, with Ditton and Farrell (2007) asking how do we measure or tap into the experience of fear? With these varying

perspectives, a sense of the importance to criminological researchers of the field of fear of crime becomes discernible.

With these established interests in fear of crime, however, the fear of cybercrime specifically has not garnered much interest. On the other hand the contemporary technological milieu with its continuous techno-scientific innovations justifies the need for a specific focus on cybercrime. Consequently, the need for such a focused study has been underscored in recent studies (Alshalan, 2006; Henson, Reyns & Fisher, 2013; Yu, 2014). It is important for a cybercrime focussed research in order to establish the degree to which established patterns in the fear of conventional crime literature relates to fear of crime (Henson et al., 2013). Even though a survey by the Mississippi State University revealed some similar patterns in terms of age, gender, experience of victimisation and perception of crime seriousness (Alshalan, 2006), Yu on the other hand argues that the study was based on a measure of cybercrime as an aggregate construct (Yu, 2014). Yu therefore calls for a disaggregation or distinction among cybercrimes to the extent of establishing fear of victimisation. Therefore in a study to test the main traditional predictors of fear of crime – perceived crime seriousness, perceived risk of victimisation and victimisation experience – on the fear of cybercrime, Yu (2014) found that fear of cybercrime does not always share the same predictors with fear of conventional crime, depending on the type of cyber crime. An additional predictor, thus internet use, was identified as also influencing fear of cybercrime.

2.7.1. Debates on and Correlates of Fear of Crime

2.7.2. Gender and Fear of Crime

The fear of crime literature reveals a gendered difference in the expression of levels of fear. The gendered difference according to Callanan and Rosenberger (2015) has been established in various studies, with evidence revealing that gender matters both as a

statistically significant control variable and especially because gender plays a central role in determining fear (Lane & Fisher, 2009). Other studies have pointed to much more directional findings in relation to the specific influence of gender on fear of crime. For example, Callanan et al. found that “women express significantly higher levels of fear in comparison to men” (Callanan et al., 2015:322). The question that comes into the discussion, in relation to this project is whether or not the fear of cybercrime victimisation also exhibits a gender differential.

In a survey at the Mississippi State University, Alshalan found that fear of cybercrime was gendered, with females demonstrating higher levels of fear than their male counterparts (Alshalan, 2006). More specific finding in the literature reveals that females were more likely to be ‘very concerned’ about online credit card theft than males (Fox, 2001). Other studies also point to gender (females) as a predictor of cyber-identity theft victims (Anderson, 2006). Having said these, it remains debatable though the extent of the occurrence of such findings. Is the finding on women’s heightened fear of criminal victimisation and specifically of cybercrimes, dependent on other factors and or under given situations or contexts? In other words, how generalizable is this finding? Some researchers have attempted a clarification of the gender-fear of crime relationship with evidence pointing to the effect that men express heightened fear as they age while women experience decreased fear, and in some cases their fear of crime is unaffected with age (Franklin & Franklin, 2009; Schaefer, Huebner & Bynum, 2006).

Meanwhile the proposition that men express heightened fear as they age has been challenged in the literature, owing to the fact significant research gaps exist with reference to knowledge about older men (Beaulieu, Dubé, Bergeron & Cousineau, 2007). Some specific gaps are in relation to the more personal and social vulnerability aspects of older men’s lives, such as victimisation, sense of frailty and insecurity among others (Beaulieu et al., 2007:337).

This finding portends far reaching consequences for older men's fear of crime. Contrary to the literature on older men's fear, studies also reveal that elderly women experience the highest levels of fear of crime, even though they are least likely to become victimised (Fetchenhauer & Buuk, 2005; Hale, 1996; Jackson, 2004; Keane, 1992; Ortega & Myles, 1987). This finding brings to the fore the concept of victimisation paradox (Hale, 1996). This concept describes the situation where, either persons with the least risk of victimisation tends to demonstrate the most fear, or persons at high risk of victimisation demonstrating the least fear. Consequently the fear of crime expressed by older women and younger persons has been explained with reference to the concept of victimisation paradox, given they each fall into the respectively scenarios.

Ferraro (1995; 1996) attempts an explanation of women's differentially higher level of fear of crime by utilising the concept of "shadow of sexual assault hypothesis". According to this concept, women's fear of rape masks their fear of other forms of victimisation (Ferraro, 1995; 1996). Also in line with Ferraro, Gordon and Riger (in Lane et al., 2009:260) suggest that being raped is an "ever-present" concern among women. Of significance here is the question how does the "shadow of sexual assault hypothesis" affect females' fear of cybercrimes? My argument here is that the sexual assault hypothesis proposition, however, is untenable for non-sexual assault related fear of crime and specifically fear of cybercrime. How, for example, do we explain credit/debit card fraud with this hypothesis? This is because this type of crime is not susceptible to geographic boundary limitations and can occur multiple times at the same time across different locations.

On the other hand, for cybercrimes of a sexual nature, for example, cyber pornography, the "shadow of sexual assault hypothesis" could become applicable. Other studies hold the view that the gender difference can be explained away by the fact that women are incapable of defending themselves in physical attack (Callanan et al., 2015; Hale,

1996). Such ‘incapability’ therefore contributes to women’s heightened levels of fear. This position however, is not sustainable with females heightened fear of cybercrime. The posturing is very simplistic and tends to assume that whereas on the one hand, all females are ‘weak’ and indefensible; males on the other hand, are ‘strong’ and capable of defending themselves in situations of physical attack. Such a position further seeks to assume that all crimes have a physical nature and consequently women expressing much higher levels of fear than their male counterparts. In the realm of the cyber world where the manifest presence of persons is absent, the argument of capability or otherwise of defending oneself in physical attack does not even arise.

However, the finding on gender and specifically females expressing more fear, is not a strongly supported one, with other studies pointing to contradictory and at times, indifferent outcomes. Contrary to the gender significant finding, Roberts et al. (2013) found that gender was a poor predictor of fear of cyber-identity theft victimisation, accounting for less than half of the variation in the fear of cyber-identity theft victimisation. Also gender (males instead of females) was a significant predictor of cyber-identity theft victimisation (Australian Bureau of Statistics, 2008). Other researchers have pointed to the fact that the gender effect is not unique but conditional. That is, it interacts with other variables to bring about an effect. More specifically, the media is identified as influencing the gender effect on the fear of crime (Callanan et al., 2015; Shrum & Bischak, 2001). Meanwhile the view that crime-related media consumption has a greater influence on women’s fear of crime has only received partial support (Callanan et al., 2015). Rendering of the media influence on the gender effect has not similarly been made for fear of cybercrime. Its applicability or otherwise in the context of cybercrime remain unanswered for now. The finding of women expressing disproportionately higher levels of fear of crime has also been challenged by feminist criminologists. Consistent with their orientation, feminists criminologists argue that gender is

socially constructed and more specifically “gender differences in child and adult socialization” is the source of gender differences in fear of crime (Callanan et al., 2015:322).

In the midst of all these debates, Lane et al. (2009) among other researchers take the safer ground by concluding there is no straightforward or simple answer regarding the question of the relationship between gender and fear of crime. Are both genders more similar or more different from each other? Significantly for the present study, it is worthwhile examining what these mean in the context of the fear of cybercrime (credit/debit card fraud) victimisation. Is it likely to follow a similar pattern of mixed outcomes or a particular gender will hold sway in terms of the direction and strength of its relationship with fear of credit/debit card fraud victimisation? The relative absence of studies into fear of cybercrime, relative to studies into fear of conventional crimes, makes answering such questions quite challenging. Does the risk society, engendered by the technological innovations of the 21st century, of which cybercrime is a significant part, disproportionately affect either gender or has an indifferent effect on both genders in relation to their fear of credit/debit card fraud victimisation?

2.7.3. Income and Race/Ethnicity

Income and race or ethnicities are further metrics used to measure their influence on fear of criminal victimisation. Findings on these metrics, like gender, are not quite straightforward. Researchers have found that the poor and people of colour demonstrate disproportionately higher levels of fear of crime (Ferraro, 1995; Garofalo, 1981; Parker & Ray, 1990; Taylor & Hale, 1986). On the other hand, these findings have been contradicted, especially outside of the realm of place-based physical crimes. The literature reveals that income and race significantly impacts people’s fear and victimisation from non-conventional crimes (Anderson, 2006; Australian Bureau of Statistics, 2008). In his study of cyber-identity

theft victimisation in the USA, Anderson found that affluent people were more likely to become victims of cyber-identity theft fraud (Anderson, 2006). On the other hand in a separate study in Australia, it was established that persons with the highest weekly incomes were more likely to be identity fraud victims (Australian Bureau of Statistics, 2008).

The contrasting findings in the above paragraph suggest the effect of income on fear is rather fluid and not consistent across board. It tends to suggest the effect of income on fear depends on the type of crime as revealed in both the USA and Australian studies. As well as the type of crime, most of the relationships among the socio-demographic variables are attributable to lifestyle as well as the condition in which residents live (Callanan et al., 2015). To this, it has been suggested that the income and fear relationship may be accounted for by differences in residential neighbourhood conditions (Skogan, 1990; 1993). Another observation about the income variable is that it interacts with other variables (cross-sectionality) to bring about given effects. For example in the case of Anderson (2006), income interacts with age and gender in exposing people to victimisation. That is, younger adults, women and affluent people were more likely to become victims. On the other hand with the Australian study, income interacts with gender, age and education to predict who becomes predisposed to the risk of victimisation. Consequently, males, aged between 25-44 years, with higher educational qualifications and with the highest weekly incomes were more likely to become victims of identity fraud (Australian Bureau of Statistics, 2008).

Given the above positions in the literature, the context of the present study is significant. What is the impact of income or affluence in determining people's fear of credit/debit card fraud victimisation? Are people living on relatively higher incomes both predisposed to and fear credit/debit card fraud victimisation more or rather, are people on lower incomes more fearful of credit/debit card fraud victimisation? These questions have not

received sufficient responses from the literature and form an intrinsic part of the analysis in the current study.

On the other hand, racial or ethnic identification also feature in the literature of predictors of fear of criminal victimisation. With regards to the racial variable, however, the literature suggests a general consensus with regards to its unique predictive effect on fear of crime. Racial and ethnic identification constitute a significant predictor of fear in the sense that persons who identify as black (persons of colour) tend to express more fear as compared to persons who identify as white/caucasian (Braungart, Braungart & Hoyer, 1980; Ferraro, 1995; Clemente & Kleiman in Parker, Mcmorris, Smith & Murty, 1993; Parker & Ray, 1990; Parker, 1988). Analysis of data from the National Opinion Research Centre (NORC) show that racial identification significantly distinguishes fearful citizens from non-fearful ones, with a relatively disproportionate percentage of middle-aged and elderly black women revealing fear of walking in their neighbourhoods (79-81%) compared to between (58-64%) of white women of all ages reporting fear (Braungart et al, 1980:61). On the other hand, younger black males (6%), young white males (21%) and young black females (38%) were the least likely to express fear (Braungart et al., 1980:61). Even though racial or ethnic identification is presented as a significant predictor variable of fear of criminal victimisation, its unique predictive impact has been moderated by age. That is to say, an element of cross-sectionality between racial identification and age is at play in determining which category of people express more fear.

The differential expression of fear by both black and white respondents has been accounted for by exposure to criminogenic conditions and resources (Parker, 1988). The disproportionally high fear by blacks is linked to the negative effects of being less educated and female or black, or being female and black or young. On the other hand, the disproportionally less fear by whites has been linked to their “limited exposure to

criminogenic conditions, having more financial resources for coping with the threat of criminal victimization, and having more confidence in the community institutions of security and justice” (Parker, 1988:491). Even though a plausible perspective, Parker’s explanation also raises several critical questions. What is the state’s response to the problem of less education by blacks or persons of colour? Is their increased exposure to criminogenic conditions a result of the social structural arrangement of the society, or is it internal to black people themselves? Why do black and other persons of colour so distrustful of the community institutions of security and justice? These are just but few of the questions which needs a thorough and critical review.

Like income previously, the impact of racial identification on people’s fear of credit/debit card fraud is a relatively untouched area. Does the finding on blacks increased fear for conventional crimes apply similarly to the field of cybercrime, and specifically credit/debit card fraud? Are there possible interactions or cross-sections with other variables? These questions among others have not gained much attention. Consequently, the present study will test for the predictive significance and direction of the racial identification variable.

2.7.4. Marital Status and Education

Marital status and education have also been studied as part of the socio-demographic correlates, with regards to their relationship with fear of crime. In relation to marital status, comparison is often made between the married and single or non-married persons, even though the non-married category is further divided into sub-categories at other times. Depending on the society and people’s orientation, marriage holds varied significance for different people. Studies predominantly reveal that married people have less fear compared to their non-married counterparts (Schaefer et al., 2006; Baumer, 1978; Braungart et al., 1980; Lane et al., 2009; Roberts et al., 2013). Significantly, the literature reveals interaction of the

marital status variable with other variables to influence people's fear of crime. From an analysis of data from the National Opinion Research Centre (NORC), Braungart et al. (1980) demonstrate that never married elderly men and women constituted the most fearful group with (80%) fear. They also found that elderly divorced or separated women (85%) and widowed women of all ages (72-100%) were more likely fearful; compared to those with a spouse (Braungart et al., 1980:60). In a related study, married and older white respondents living in a household with others, or living in urban areas expressed less fear of criminal victimisation (Parker, 1988). The two studies reveal different intersections of marital status with other variables to influence fear in particular directions.

Married persons reduced fear has been traced to companionship and its effect on reducing vulnerability (Parker, 1988). Married people according to this view, enjoy the companionship of their partners which reduces feelings of loneliness, and culminates into reduced feelings of vulnerability. Accounting for marriage in this way however, can be problematic. The fact people go into marriage for different reasons have not been factored into the explanation.

On the other hand, education as a socio-demographic variable is seen as important in determining people's socio-economic status, and consequently is also linked to whether people have more or less fear of criminal victimisation. Persons with high or more education tend to express less fear of crime compared to their less educated folks (Baumer, 1978, Lane et al., 2009; Schaefer et al., 2006). And as previously seen under marital status, education also interacts similarly with other variables to influence fear of crime. For example the married and highly educated people demonstrate lower levels of fear of crime compared to single and less educated people (Schaefer et al., 2006; Baumer, 1978). Parker's concept of limited exposure to criminogenic conditions, resources to cope with threat of victimisation

and trust in the justice system may very well explain the reduced fear by highly educated persons (Parker, 1988).

It is important to point out that the above findings so far are in the realm of conventional crimes. With regards to fear of cybercriminal victimisation, whereas marital status and education have not been supported as significant predictors of fear of victimisation (Roberts et al., 2013), on the other hand, education is supported as a significant predictor of fear of cybercrime (cyber-identity theft fraud) victimisation (Australian Bureau of Statistics, 2008). These findings as revealed constitute an important step in the study of fear of cybercriminal victimisation. However, not much of such focused findings have been revealed for credit/debit card fraud victimisation. The current study on credit/debit card fraud will therefore make an important contribution to the body of knowledge of fear of cybercriminal victimisation literature.

2.7.5. Vulnerability

Social and physical vulnerability also constitutes correlates of fear of crime. Vulnerability relates to feelings of insecurity or safety within an individual's surrounding, be it household or neighbourhood. Social and physical vulnerability suggests the incorporation of both individual and community aspects to why and how people come to have fear of crime (Hale, 1996). This view ties into Schaefer et al. (2006) earlier point on perceptions of disorder in one's neighbourhood. The neighbourhood context has an influence on fear of crime, with the general argument that socially integrated neighbourhoods foster support and thus reduces fear of crime among residents (Hale, 1996). Silverman and Kennedy (in Callanan et al., 2015) observed that individuals living alone have higher levels of fear of crime compared to those with close social ties. However the extent of influence neighbourhood context has on fear of crime is not immediately clear from the argument.

The argument that persons living alone are more than likely to express higher levels of fear is untenable within the context of an increasingly technocratic and individualised world. This is especially true of the developed western world and sustaining this argument would mean people in these environments have no choice but to perpetually live in conditions of fear. My perspective here is that the view is highly debatable. Within the context of a risk society and flowing from technological innovations, vulnerability in terms of social and physical context will have very little, if any influence on the risk or fear of cybercrime victimisation. My argument is that the marker of vulnerability in this context stems from ones activities on the internet (exposure to computer systems).

2.7.6. Experience of Victimisation

Prior experience of victimisation remains a much studied correlate of fear of crime. The findings here too are unsettled. Previously held dominant view was that crime victims have the potential to more than likely express higher levels of fear of crime. Researchers from this perspective held that there was a positive association between victimisation and fear of crime, with victims of crime expressing relatively more worry and perceiving more risks (Friedman et al, 1982; Mawby and Gill, 1987; Maguire & Corbett, 1987, Smith & Torstensson, 1997). In their Australian study, Mawby and Gill found that fear was the commonest emotional response experienced by victims of crime (Mawby et al., 1987). Significant at this point is the question does the experience of victimisation influence fear of cybercriminal victimisation? The literature has contrasting responses. Persons with experience of victimisation demonstrate higher levels of fear of cybercrime victimisation (Alshalan, 2006). On the contrary Yu (2014) argues that the predictive influence of experience is not straightforward and depends on the type of cybercrime at issue.

Subsequent research has tended to question the dominant view of experience in relation to fear of crime (Callanan et al., 2015:324). Some studies argue differently by

demonstrating that fear is unrelated to patterns of victimisation or actual victimisation. Instead according to these researchers, fear of crime is the result of “perceived vulnerability based on subjective judgments of personal risk.” (Whitrod and Maxfield, in Carcach et al., 1995:273). This perspective resonates well with the perception of disorder argument. Consequently it goes to question the broader theme of fear of crime. On the other hand, Rosini (in Carcach et al., 1995) also argued that previous victimisation, rather than increase fear of crime tends to motivate people into taking precautionary measures and thus lessens their fear of crime. This latter argument is however questionable. Significantly the idea of taking precautions could as well be interpreted to mean harbouring fear, the reason for which an individual resorts to those measures. This is because the relationship between the two (adopting precautionary measures and fear reduction) is not linear or causal. Precautionary measures in this regard can be seen more as a risk mitigating step. From the foregoing review, it is apparent that not much work has been done on the relationship between experience of victimisation and fear of cybercrime victimisation. This research will contribute to filling that void by exploring the theme.

2.8. Measuring Fear of Crime

Measuring fear of crime has attracted as much controversy, if not more than the predictors of fear of crime. Even though the importance of fear of crime is not in doubt, the question of an acceptable medium to measure it remains a challenge. The quantitative methodology, and specifically the survey design, is the predominantly used approach (Hale, 1996; Farrall et al., 1997, 2004; Yang & Wyckoff, 2010). However the survey method is critiqued as not being the best for measuring fear, with the argument that it leads to an exaggerated emotional response (Farrall, 2004). Instead, for Farrall (2004), ethnographic and qualitative data reveal that people have less common experience of fear or anger of crime victimisation. The continuing doubt over the feasibility of the survey method has led to

persistence in the argument that the prevalence of fear of crime is misrepresented (Farrall et al., 1997:659). Therefore given these views, it is concluded that our understanding of the fear of crime is a result of the way it has been measured and not its objective occurrence (Farrall et al., 1997).

Fear of crime is also measured in two broad approaches; thus individual self-report and by monitoring physiological processes associated with fear (Warr, 2000). The approach utilised depends on the given situation as well as the orientation of the researcher. Both approaches have their unique strengths and limitations. Physiological monitoring, for instance allows for measuring fear as it occurs, that is, through a natural and unhindered occurrence in real time and natural settings (Warr, 2000). It also eliminates problems with self-report such as recall, demand effects, or reluctance to disclose emotions (Warr, 2000). On the other hand whereas physiological monitoring lacks the ability to reveal the source of fear, it also cannot distinguish fear of crime from other forms of fear e.g. accident, threatening or bad weather (Warr, 2000:456).

Related to measurement is the need to distinguish between fear of crime and related constructs such as perceived risk of victimisation as well as anxiety. This is because most of the arguments regarding the appropriate medium of measurement stem from a lack of agreement of what fear of crime is and what it is not. As the temptation to equate fear of crime with perceived risk of victimisation represents a challenge to criminologists attempt at defining fear (Warr, 2000), the distinction between the two constructs has consequently become an important contribution to the field of fear of crime studies (Mesch, 2000). Ferraro defines fear of crime as “an emotional response of dread or anxiety to crime or symbols that a person associates with crime” and perceived risk as “recognition of a situation as possessing at least potential danger, real or imagined” (Ferraro, 1995:4). Therefore fear is not perceived risk; rather it is its consequence (Hale, 1996; Warr, 2000). This suggest that most fear of

crime surveys end up measuring perceived risk and not fear of crime. As a result, Hale suggests that “measures of fear of crime should tap the emotional state of fear” and should include such terms as “how afraid” or some similar phrases (Hale, 1996:93).

The literature further makes a distinction between fear and anxiety; the former referencing reactions to immediate and intense danger, and the latter reactions to future or past events (Warr, 2000). However, whereas most people mean "fear" in reference to fear of crime, most measures of fear are actually designed to capture anxiety, rather than fear of victimization (Warr, 2000:454). However, once again are these distinctions always as clear cut? Are the distinctions even necessary? The underlying fact is they both constitute emotional reactions to given cues. The distinctions as suggested above can at best be confusing.

2.9. Chapter Summary

This chapter has presented the literature review of some key themes and debates in the study of cybercrime and fear of crime. The chapter began with a review of general themes in white-collar/corporate crime and cybercrime victimisation. The rationale for this was given as providing conceptual and theoretical clarity right from the beginning. Next the chapter examined literature on the various key debates such as defining cybercrime, the criminological quandary and the relationship between technology and cybercrime. Understanding these debates is deemed necessary to understand the focus of the thesis. Given there are several types of cybercrimes and the confusion with other crimes, the chapter also examined the characteristics as well as types of cybercrimes and the terminological differences. In order to assess the level of seriousness of the problem of cybercrime, the chapter also reviewed literature on the prevalence of cybercrime and specifically, credit/debit

card fraud. The chapter then turned its focus onto fear of crime, correlates or predictors of fear of crime and ended with measuring fear of crime.

CHAPTER 3

THEORETICAL FRAMEWORK

3.1. Overview/Introduction

The focus of this section is to provide a brief background to my research with an emphasis on the theoretical literature review. As a starting point, cyberspace has increasingly changed the nature and scope of criminality (offending and victimization) and thus represents a new frontier for criminologists, even though they have acknowledged but have been slow in reacting to it (Jaishankar, 2008). This partly explains the relative lack of depth of theoretical explanations for cybercrime with previous theories unable to fully account for the ever changing dynamics of cyber criminality. Fear of crime on the other hand has generated much research interest among criminologists. As a result of such interests, criminologists have sought to understand the various elements and influences on the fear of crime among other themes. The established interest in fear of crime, however, has been focused on physical or conventional place-based crimes. The fear of cybercrime specifically has not garnered much research interest. Statistics reveal a rising concern and fear of victimisation of various cybercrimes. More specifically, cross-country data reveals a rising trend of concern for credit/debit and bank card fraud among people (Fox, 2001; Australian Bureau of Statistics, 2008; Roberts et al., 2013). The above therefore represents one of the bases for my interest in the subject matter.

The rest of the chapter will proceed by first reviewing some previous attempts by socio-criminological theories in explaining fear of crime. The theories to be reviewed here include the vulnerability thesis, the instrumental thesis, the incivilities thesis and psychological factors. Following this, the chapter will proceed to examine the substantive theory for this thesis - Beck's theory of Risk Society – together with some of the criticisms

labelled against Beck's theory. From here on the chapter examines some works of contemporary sociologists on risks including Luhmann and Giddens. Finally, the chapter presents general reflections from the Risk society theoretical framework. The chapter ends with a summary of the discussion.

3.2. Explaining Fear of Crime (Socio-Criminological Theories)

The transformations and prevalence rates of crime, and especially people's reaction to them have occasioned the need to find theoretical explanations for the problem, as well as people's reactions to it. However, the nature of cybercrimes has made it difficult to utilise typical classical agency and structure based theories. Previous attempts have been made by scholars to explain the broader theme of fear of crime without specifically narrowing down on fear of cybercrime victimisation. The review below therefore looks at some of these theoretical attempts at explaining fear of crime and examining their applicability to the risk of cybercrime (credit/debit card fraud) victimisation. The review will conclude with observations and lessons from the theories collectively. My intention in this project, however, is to utilise the postmodernist theoretical framework of "Risk" Society by Beck (1992). It is hoped that this framework will be a much better fit in efforts at understanding the fear of cybercrime victimisation, given the inevitability of the consequences of technological transformations and the shift in the overall social and technological contexts in which individuals have been positioned.

Generally, four theoretical explanations have been identified in accounting for fear of crime (Hale, 1996). These include:

1. Vulnerability thesis
2. Instrumental thesis
3. Incivilities thesis

4. Psychological factors

3.2.1. Vulnerability thesis

Vulnerability relates to notions of helplessness in a given situation. In this case, criminal situations give rise to feelings of fear or otherwise. Hale (1996) presents a common sense perspective of vulnerability that when people feel unable to protect themselves – for a variety of reasons including inability to run fast or lacking the physical prowess to ward off attackers among others – they may be expected to fear crime more than others (Hale, 1996). Three identifiable groups as a result fall into this category namely women, the elderly and the poor (Hale, 1996). The vulnerability thesis has been approached differently by a number of authors, with each including various elements in her/his conceptualisation of vulnerability. Killias (1990) for example adds extra dimensions of physical, social and situational components to his vulnerability framework. Conceptualised this way, the vulnerability thesis represents a classical structure argument with humans as agents, being given to the dictates of structure. In other words, human beings lack agency and for this reason, are unable to proactively affect the environment around them.

Generally, the vulnerability perspective is especially tied to the gender effect argument as a correlate of fear of crime. According to most studies, the gender effect, which suggests females are more likely to express higher levels of fear of crime, has proven to be a consistently robust finding (Callanan et al., 2015; Schaefer et al, 2006). However other studies have come to challenge this overly dominant view. Even though supported by some scholars, it is argued gender on its own has no such strong impact on fear. That is to say, gender has a conditional effect on fear of crime and only becomes strong in interaction with other factors, such as the media. Feminist criminologists on the other hand have challenged this thesis, arguing that gender is socially constructed and thus differences in socialisation

account for the gender effect in the fear of crime (Callanan et al., 2015). Hale also alludes to the role of socialisation in his review of Killias' when he cautions that perceptions of vulnerability may be influenced by processes of socialisation and hence, the need for caution in arriving at conclusions and generalisations (Hale, 1996).

The vulnerability thesis as outlined above, could potentially only partially account for the fear of cybercrime victimisation. The common sense explanation of inability to protect oneself in physical attack is inapplicable for cybercrime victimisation, as these crimes do not involve the physical presence of offender and victim. The gender, age and income variables as seen in women, the elderly and the poor, are not unanimously supported as being much more vulnerable and hence having much fear of cybercrime victimisation. Gender which seems to have been relatively supported has also come with mixed findings. Whereas females have been supported to demonstrate higher levels of fear of cybercrime generally, and specifically, cyber-identity theft and credit card fraud respectively (Alshalan, 2006; Anderson, 2006; and Fox, 2001), males on the other hand demonstrate higher level of fear of cyber-identity theft victimisation (Australian Bureau of Statistics, 2008). On the contrary both of the above outcomes have been challenged with the finding that gender is not a significant predictor of cyber-identity theft victimisation (Roberts et al., 2013).

Therefore given that cybercrimes and more specifically, credit/debit card fraud are committed through online media, where the physical presence of offender and victim is not needed, vulnerability as reflected in socio-demographic variables can only be of minimal explanatory power. Unlike in physical place-based crimes, vulnerability to cybercrime victimisation may only partially be explained or enhanced by one's exposure to the internet and other computer systems.

3.2.2. Instrumental Thesis

The instrumental thesis relates to people's experiences of crime, either directly or indirectly through the experiences of friends, family or other significant others. The ready conclusions flowing from the common sense expectation of a direct relationship between victimisation and fear of crime is not that straight forward and has resulted in varying outcomes (Hale, 1996). Though the experience of criminal victimisation may result in a person becoming more cautious (Carcach et al., 1995), it is unclear whether such caution consequently make a person more fearful (Hale, 1996). Whereas some studies have found evidence in support of the direct relationship between victimisation and fear, others have presented evidence pointing to a weak relationship and still with others finding a non-existent relationship (Box et al., 1988; Braungart et al., 1980; Liska et al., and Wanne & Caputo in Hale, 1996: 104). However the argument that experience of crime make people more cautious and hence less fearful of crime is untenable. The same argument could as well be interpreted to mean such a person is harbouring fear, and thus the reason for such cautious steps.

Indirect victimisation and fear of crime has also thrown up mixed findings in terms of their relationship. Whereas some literature has found evidence suggesting indirect victimisation is statistically significant using global measures, it at the same time found indirect victimisation as insignificant when using crime specific questions (Box et al., 1988). On the other hand, in a comparative study of data on fear from three surveys, Arnold (1991) did not find support for the significance of direct victimisation. Instead he found that "indirect (vicarious) victimisation contributes significantly to the prediction of fear within all three surveys (Arnold, 1991: 118). The effect that indirect victimisation has on fear of crime is mediated by other factors notably the media, and more specifically television (Callanan et al., 2015). Using what is called the "Substitution Hypothesis", Gerbner, Gross, Morgan and Signorielli (1980) elaborate on the specific effect media has on fear of crime. Their

hypothesis states that people establish opinions about crime from media representations as a way of substituting for their lack of personal experience with crime (Gerbner et al., 1980). This hypothesis is significant in contributing to our understanding of what Hale (1996) term the “fear-victimisation paradox”; that is, the situation where people with the least risk of victimisation express heightened fear. This is particularly the case with the elderly and women. On the other hand, utilising what they call the “Affinity Hypothesis”, Chiricos, Eschholz, and Gertz (1997) argue that the media effect on indirect victimisation is especially pronounced when viewers are demographically similar to crime victims on the television. The conclusion drawn from the above is that the indirect victimisation-fear relationship, like the direct victimisation-fear relationship is inconsistent and conditional in most instances, as seen with the media.

Various explanations have been put forward to account for the inconsistent findings in the victimisation-fear relationship. In all of these explanatory attempts, however, Hale argues that the use of global measures rather than crime-specific measures is a very strong possibility (1996). Hence this current project finds support with Hale’s observation.

In the context of credit/debit card fraud victimisation, the applicability of the instrumental thesis could be explored. This is despite the mixed findings of the relationship between prior experience of cybercrime victimisation and fear of cybercrime victimisation (Alshalan, 2006). It may sound reasonable to expect that a person having had experience of cybercrime victimisation, either a direct first-hand experience or indirectly through a friend or significant other, may be much more fearful of subsequent victimisation. Reasoning this way offers greater possibilities given that unlike physical place-based crimes, cybercrime and specifically credit/debit card fraud is not affected by physical proximity and with perpetrators enjoying an almost perfect anonymity. The resultant air of uncertainty in relation to when and how a person may become victimised could likely make persons with victimisation

experience (direct or indirect) to become much more fearful of the risk of subsequent victimisation. So rather than experience of victimisation motivating people to become more cautious as Carcach et al. (1995) argues, the experience could actually make such persons more uncertain and hence fearful of subsequent victimisations.

The “substitution hypothesis” explanation of the media influence on indirect victimisation on fear of crime could as well be applicable to cybercrime victimisation. Unlike explaining the fear exhibited mostly by the elderly and women, however, it can in this case apply to any given person who has or is affected by media presentations. The “affinity hypothesis” on the other hand may not be applicable with cybercrime victimisation given the absence of physical proximity as well as the anonymity of perpetrators. This is because the affinity hypothesis refers to viewers sharing demographic similarity with crime victims. And following from Hale’s (1996) view that the use of global measures rather than crime specific measures could account for the inconsistencies in the victimisation-fear relationship, this project which is focussing on cybercrimes and specifically credit/debit card fraud, hope to be able to make a contribution toward clarifying the raging debate.

3.2.3. Incivilities

Incivilities relates to the condition or nature of the local environment - both physical and social - in which a person lives and not so much about the actual prevalence of crime. The neighbourhood argument finds expression and support with this thesis. The proposition includes the idea that physical deterioration and social disorder of neighbourhoods accounts for people’s fear of crime in a given neighbourhood (Hale, 1996). Socially cohesive neighbourhoods by this reasoning foster safety and thus less fear of crime. Gossip and rumour especially in integrated communities serve a useful function of information dissemination on the prevalence as well as the source and intensity of potential danger

(Merry, 1981; Yin, 1980). The information dissemination role is therefore central to when and whether people experience heightened levels of fear based on the presence of criminality at any given time. This theory has a ready application to fear of physical place-based crimes because of the aspect of physicality.

On the other hand, the incivilities framework also has a possible application – albeit limited - with cybercrimes. This is because there is a cyber equivalent of disorderly social environments. For example there are numerous intrusive evidence of trolling, proliferation of pop-ups for no apparent reason, spamming (particularly for unsavoury sites) among others on the internet platform. These evidences of intrusion significantly raise doubts and fears about the safety of financial information. As credit/debit card transactions involve dispensing with crucial identifying and financial information, internet patrons can generally be expected to be wary and fearful of becoming victimised. To that extent, the incivilities thesis can be of useful explanatory value to why and how people express fear of credit/debit card fraud victimisation.

Due to non-physicality in cyberspace, however, the neighbourhood context has a generally different application. Consequently the incivilities thesis is somewhat at variance with and incapable of significantly accounting for fear of cybercrime victimisation. This is because the social and physical environment has no immediate application in cyberspace. As outlined earlier, among the defining features of cybercrime include the fact that it is unaffected by the physical constraints dictating activity in the physical world, it does not require proximity between the victim and the offender and as well perpetrators enjoy almost perfect anonymity among other features. This underscores the limited explanatory significance of the incivilities thesis. The point being that even in regard to physical crimes, we live in an increasingly individualised world system, more so the case in the western world, with there being no indication of an imminent retreat of the current situation. Even the

developing world which is generally seen to exhibit high sense of mechanical solidarity (in the 'Durkheimian' sense) is increasingly experiencing social change, significant part of which leaves its inhabitants increasingly individualised (Abotchie, 1997; Nukunya, 2003).

3.2.4. Psychological Factors

Fear of crime has been looked at from two dimensions within the psychological realm (Hale, 1996). It is viewed as "an emotional response to signals of danger in the environment while to others it is a manifestation of a general uneasiness about the world" (Hale, 1996: 120). These dimensions immediately bring to mind the question whether fear is a consequence of crime or a precursor to crime. Hale has referred to this as causing a causal ambiguity as with other measures (1996). However unlike the previous theses, psychological factors have not engendered a great research focus among researchers and with most researchers looking at it under a general modelling framework (Hale, 1996). The effect of this is that there have not been robust findings with the relationship between psychological factors and fear of crime. Most of the findings according to Hale (1996) have pointed to weak associations.

Even though it has not generated much research focus with physical place-based crimes, psychological factors could have some explanatory significance for fear of cybercrime (credit/debit card fraud) victimisation. Fear of credit/debit card fraud victimisation could be the result of either or both of the dimensions of psychological factors as suggested by Hale (1996). That is, either as an emotional response to signals of danger in the environment or a manifestation of a general uneasiness about the world. Danger and uncertainty in the cyber landscape (environment) resulting from technological innovations could potentially lead people into having fear for cybercrime victimisation. Conversely the uneasiness in the world resulting from the unintended consequences of continual

technological and scientific advancements could as well lead people into being fearful and overly conscious of credit/debit card fraud. Therefore seen from these dimensions, psychological factors could be of some useful explanatory value for fear of credit/debit card fraud victimisation.

Following from the review of the above theoretical attempts at explaining fear of crime from the various perspectives, and their potential applicability to fear of credit/debit card fraud, two observations can be made. The first observation is, that the suggested theses (theoretical positions) constitute general propositions to explaining mostly broad based ‘ordinary’ street or place-based crimes. The second observation is that previous studies on the fear of crime have almost always used global measures without narrowing down on specific crimes. This has therefore accounted for the lapses in those theories applicability to fear of credit/debit card fraud victimisation. These observations are significant and provide a critical niche for the direction of this current project. Specifically, the focus of the present study is drifting away from theories focussing on specific cases of fear of crime as discussed above, towards a shift in the overall social and technological context in which individuals, as reflexive agents, are positioned. The shift in theoretical focus is essentially grounded in the prevailing social and technological milieu of late modernity. The shift in social and technological contexts which give rise to separation of time and space of the offence in cybercrime, also changes the psychology of fear. Invisible dangers can be both easier to ignore, but once fear is activated, more terrifying than dangers.

3.3. Theory of a Risk Society (Beck, 1992)

Beck’s theory of risk society is one of several sociological attempts at making sense of the contemporary era and the challenges embodied in it. Following in the steps of the sociology of science and knowledge, Beck’s theory is very critical of scientific knowledge and advancement. Beck’s risk society embodies two central theses, that is, reflexive

modernisation and risk (Beck, 1992). In light of the many unintended consequences occasioned following the numerous breakthroughs in techno-scientific innovations and development, the prevalent contemporary situation has been termed a ‘world risk society’ (Beck, 1996). The main argument in risk theory is about the centrality of ideas of risk given the various scientific developments in the world order. Instead of the usual generally benign outlook on scientific achievements, Beck’s theory argues for a critical perspective on the ‘progressive’ role of science and technology. The “consequences of scientific and industrial development are a set of risks and hazards, the likes of which we have never previously faced” (Beck, 1992:2).

A major and recurrent argument in the sociology of science and knowledge is that scientific knowledge is not pure and is a set of social relations. As a result of this argument, Beck’s theory is therefore seen to have origins in the sociology and critique of scientific knowledge (Beck, 1992). Dangers resulting from the various technological and industrial developments are not limited in time and space. A significant feature of risk society according to Beck is that unlike in previous epochs, none can be held accountable for the hazards of the ‘risk’ society. People living in this society lack a definite idea of the extent of risk facing them, consequently it becomes difficult to compensate victims of these hazards. These basically constitute Beck’s idea of risk. Therefore seen in this light, cybercrime, which is a by-product of advancements in technological and scientific innovations, rightly falls under the spectrum of the risk society. As criminal activities aided by the use of computers (both as a tool and object), cybercrime defies boundaries and time limitation as they can be committed simultaneously across multiple locations. In Beck’s language therefore, the dangers of cybercrime (credit/debit card fraud) as a consequence of technological innovations, is not limited in both time and space.

In the midst of the gloomy picture painted of the current global dispensation, however unlike Weber, Foucault or Adorno, Beck is not overly pessimistic about the situation (Beck, 1992). He instead argues that the *effets pervers* of modernisation can be managed through the radicalisation of the new rationalisation, which calls for reflexivity as an important element in the evolution of societies (Beck, 1992). As well, reflexivity, above all, means self-confrontation (Beck, 1996), elements of which are, for example, already observable in the green movement which is seen as a critique of science. For Beck, modernisation involves both a structural change as well as changing relationship between social structures and social agents. At a given stage in the modernisation process, the relationship between social structures and agents become highly individualised, and agents become less constrained by structures (Beck, 1992).

The risk society is a distinct social formation working on radically different axial principles (Beck, 1992). The axial principles of risk society are the distribution of “bad’s or dangers” and the society is structured through individualism (Beck, 1992: 3). Individualism is therefore an essential part of the risk society. Successful modernisation, as a result occurs when agents release themselves from structural constraint, to actively shape the modernisation process. This analysis implies there has been a radical shift in the overall social context in which individuals, as active agents, have been positioned in late modernity. The analysis also produces an interesting convergence with the work of Giddens on modernisation. Giddens makes the argument that humans (agents) are not social dopes but rather they play an active role in the construction of social reality and existence. This essentially is the idea behind Beck’s own conception of reflexive modernisation.

Beck also demonstrates stage or evolutionary tendencies in his approach. Social change is composed of pre-modernity, simple modernity and reflexive modernity (Beck, 1992). As a result according to him, whereas modernity is coexistent with industrial society,

reflexive modernity on the other hand, is coexistent with risk society. In earlier stages of modernity, progress and science were upheld with risks justified as progress and science as constituting a part of the solution rather than the problem (Rasborg, 2012). In the contemporary period, however, Beck's theoretical position suggest that the benign outlook on science and risk as constituting progress has been replaced with a more thorough and critical perspective. Science contributes to the production of risks, hence risks can no longer be legitimated by science and progress (Beck in Rasborg, 2012:14). Implicit in this discussion is the idea of an emergence of a radical shift in the technological context in which people are positioned in late modernity.

Using this theory as a framework, critical aspects of cybercrime victimisation can be understood. As individualism has become an important part of the risk society, it serves to reason that broad based categorisations of agents (individuals) and consequent generalisations in respect of these agents is inconsistent in the view of the theory. People choose to go online based on their need at any given point in time. Meanwhile there is as yet no system of governance of the activities on the platform, however, while the need to use the internet increasingly becomes inevitable on a daily basis due to the nature and demands of the globalised world today. Consequently the risk of cybercrime is a realistic possibility for any person, irrespective of gender and other socio-demographic features, choosing to use the platform. However the system of organised irresponsibility ensures no institution take responsibility for the harms visited on users of the interface. As reflexive agents in the risk society, however, users of the internet are expected to modify their behaviours, and that may mean taking precautionary steps, to successfully use the internet. Doing this will constitute a way of releasing themselves from the structural constraint (the realistic threat of cybercrime) and thus shaping the modernisation process to desired ends. In the overall analysis, Beck's theory which, argues to the effect that there has been a drastic shift in the overall social and

technological context in which individuals are positioned in late modernity, has informed the context of the present study.

3.3.1. Criticism of Beck's Risk Society theory

Beck's theoretical position has attracted some criticisms, similar to all other scholarly work. Significantly it is critiqued that risk is nothing new, for humanity has always been confronted with various kinds of risk, from earthquakes, floods, plagues, cholera among others (Rasborg, 2012). The argument goes further that not only is risk not new, but that life today is less risky in some ways than before; for example reported increase in life expectancy in most of the industrialised world demonstrates the fact that life today is less risky and more predictable (Rasborg, 2012:5).

My response to the above is that Beck's argument does not imply that risk is a novelty. Rather Beck's argument is that risk has become so widespread and assumed numerous dimensions because of the technological milieu. Risk in the (world) risk society has moved from the realm of involuntary and accidental to voluntary and human orchestrated. Risk in late modernity for Beck is 'system' immanent and universalizing, that is, all encompassing (Beck, 1992). As a result of the increased technological context, risk has become embedded into the system and has become almost inescapable. Rasborg's contention, that life is less risky in the cotemporary period is suspect. Incidents which seemingly appear less risky and predictable, invariably turns out to be very risky and less predictable with incalculable losses. The recent example of the nuclear reactor explosions in Japan underscores this position. The cyber interface where most activities take place in the contemporary period, exposes internet patrons to a whole set of challenges and risks (both old and new). The argument is not suggestive that people did not already have challenges with fraud. However, the internet which has revolutionised activities, for example banking and purchase transactions, has brought people more closely to the doorsteps of risks.

Furthermore, other scholars contend that Beck's view of risks as mainly resulting from techno-scientific development is too simplistic, arguing that, "the genealogy of risk is much more complex than the theory of risk society allows. Risks and its techniques are plural and heterogeneous and its significance cannot be exhausted by a narrative of a shift from a quantitative calculation of risks to the globalization of incalculable risks" (Dean, 1998:34). However a simple response to this criticism is that it is not a very true reflection or alternatively, it is an equally simplistic criticism of Beck's theory. Beck's argument is that the nature or extent of the risks in contemporary times (world risk society) has only been exacerbated by techno-scientific developments, which has ensured its transformation from calculable and predictable risks to incalculable and non-predictable risks. This essentially, is what Beck argues; that techno-scientific development has ensured that risks which hitherto was predictable, is no more calculable and predictable. Consequently the social and technological context has changed.

3.4. Some Contemporary Sociologists on Risks

3.4.1. Luhmann: Distinction between Risk and Danger

Several other contemporary sociological theorists have also examined risk, with Luhmann being one of those. In his view, risks are decisions observed with respect to the future (Luhmann in Rasborg, 2012). And as decisions are aimed at the future, it carries with it probabilities, hence the possibility or risk of unintended consequences of action (Rasborg, 2012). In this way therefore, all decisions, including decisions concerned with safety, are connected with risk (Luhmann in Rasborg, 2012). The implication from this position is that even safety has risk built into it. Luhmann therefore conceives of risk within the framework of risk/danger.

Following the above, Luhmann's view of risk is couched as a product of the one who makes decisions (Rasborg, 2012). Whereas for the decision maker, the consequence of action

is risk, for the one affected by such decision, the consequences appear as a danger (Luhmann in Rasborg, 2012). Luhmann's perspective affords risks a highly subjectivist element, for which reason what constitute risks in one dimension could at the same time be termed danger, based on the subjective prerogative of social systems. What is seen as risk is only but a "symptom of the way contemporary society observes itself with respect to the consequences of an increasing complexity of decisions" (Rasborg, 2012:7). Luhmann's position here is therefore consistent with his system theoretical framework and his view that social systems are self-referential.

Luhmann's perspective though is not far off from Beck's. Beck's view that risks in the world risk society (late modernity) are voluntary, artificial and system produced, implicitly affords decision a crucial role in the unfolding of risks. Again Luhmann's view, that decisions have the possibility of resulting to risks as unintended consequences, easily fits into the thrust of Beck's theory. The essence of Beck's position is the contention that risks essentially are unintended consequences of techno-scientific development. Therefore the decisions made in the drive at the massive developments in science and technology has resulted into unintended consequences as seen in the ozone depletion and in relation to the present study, cybercriminal (credit/debit card fraud) activities. In the contemporary society, the reality for most people is that banks have moved their information storage and data manipulation onto computers and computer systems. As a result, even if a person "chooses" not to bank online, they are still vulnerable as a result of decisions made by others. Their pay for example is deposited directly online. So even if they go in person, to the bank physically to make all transactions, they still bear risks from decisions made by the banks, employers and so on. It is in this context of generalised cyber-risk that the decision as to whether to expose themselves to dangers arising from their own transactional decisions is not made by individuals.

However Luhmann's perspective, wherein he attempts a distinction between risk and danger can be critiqued. Luhmann's distinction represents only an arbitrary distinction. This position is informed by the fact that risk in the (world) risk society (late modernity) is such that even decision makers are not spurred from the ever flowing and all-consuming risk resulting from techno-scientific advancements. The overall social and technological context of late modernity does not offer much choice in terms of who becomes vulnerable to risks, be it decision maker or decision taker. The difference, as Beck has repeatedly argued, is reflexivity. In the world of cybercriminal (credit/debit card fraud) victimisation, reflexivity is particularly important in distinguishing persons who move from the threshold of risk and vulnerability to actual victimisation. Given that all users of the internet, especially as far as online banking and purchasing transactions are concerned, are potential victims of credit/debit card fraud, Beck's theoretical framework of the risk society therefore offers a very useful convergence for the direction of the present study.

3.4.2. Giddens on Risk

Like Beck, Giddens view risk as a modern phenomenon and the product of human action or intervention in nature (Giddens, 1999). For Giddens early modernity was dominated by 'external risks', that is, calculable risks mainly independent of human action. However with contemporary times, risks and uncertainties have become the result of the activities of active and dynamic human agents in late modernity (Giddens, 1998; 1999).

And like Beck again, Giddens perspective is that pre-modern dangers and external risks have been replaced by a 'manufactured uncertainty' in late modernity; "... an existential uncertainty found in societies where traditional certainties are eroded as a consequence of the 'end' of tradition and the 'end' of nature." (Giddens, 1994:78, 152, 219). Giddens position implicitly points to a change in the social context in late modernity, giving rise to uncertainties, and in this case, risks. In this way, Giddens and Beck share the same or similar

position on the origin of risk in late modernity. Beside agreeing that risk is a feature of the contemporary era (late modernity), both theorists also point to a change in the nature of risks as experienced in early modernity or the industrial era and that experienced in today's late modernity. Significantly both theorists trace risk to a common thread, that is, human intervention as well as changes in the social context within which individuals find themselves.

Furthermore Giddens (1998) agrees with Beck that a feature of the risks in late modernity is their non-calculability (unpredictability). Consequently Giddens argues that risks cannot be managed through insurance (Giddens, 1998). Significantly, Giddens perspective on the impossibility to manage risk insurance-wise is particularly distinctive and "Becksian" as it clearly draws a line between risks as experienced in early modernity and in the contemporary era (risk society).

Having agreed with Beck on the foundation of risk, however, Giddens takes a different route in respect of the implication of such risks in late modernity. Giddens point of departure from Beck is his argument that the new structure of risks does not mean an increase of risks in late modernity relative to early modernity (Giddens, 1994; 1999). Instead for Giddens, it suggests that "late modernity is characterized by a change of the 'risk profile', from dangers determined by nature to man-made risks" (Giddens, 1994:4; 1999:36). On the contrary Giddens decision to not come forthright in terms of intensity of risks in late modernity leaves his theory incomplete. Does the change in profile as Giddens argue, indicative of a trend in either direction? Does the change in the risk profile then suggest risk has remained at a neutral level? The latter seem reflective of Giddens even though it is not stated in categorical terms. Indeed with the waves of technological and scientific advancements, the argument that the risk profile has consequently changed is very plausible. But to stop at just that leaves a theoretical gap. This is because with a change in the risk

profile, there should be a clear indication of whether that means risks has remained the same, increased or decreased. Beck has rightly answered or filled this gap with his position that the various changes in risks in late modernity mean an increase in risks (Beck, 1992). Once again, this categorical stance of Beck's theoretical framework in terms of the intensity of risks in late modernity, underscores the adoption of his theory for the present study. The present study therefore from the onset, adopts the position that risks in contemporary society have increased drastically, and such increment is informed by the massive transformations in science and technology.

3.5. Reflections from the Risk Society Framework

Analysis of the broad themes of Beck's risk society framework provides an important lead-in to the context of my present study. An important aspect of Beck's theory is, about the radical shift in the overall social and technological milieu of late modernity. The latter shift is, particularly significant for the current study, given the imperativeness of technology to late modern life. Analysis of Beck's risk society has also thrown up interesting observations which are intrinsically linked to the focus of the present study. These observations include:

- Existential realism of risk - risk in the modern era is inescapable, no matter a person's characteristics (gender, age, income etc.). In the context of cybercrime (credit/debit card fraud), the risk is open to all patrons of the internet. Hence the fear of cybercrime victimisation among users of the internet should normally not be gendered or exhibit much structural differences, if any. That is to say, it ought not to produce gender and other structural differences. This observation is an important lesson from Beck's theory and constitutes a major dimension of the current study.
- Individualism – individualism goes hand in hand with risk society which is coexistent with reflexive modernity. Consequently individuals are unique in both of their motivations as well as actions on the internet. Individualism is also linked with

widespread risks. Broad based generalisations and conclusions based on the activity of an individual or a given gender is, therefore not in sync with the theory. Once again an important lesson is revealed in this observation. In the face of widespread risks resulting from technology, people still act as individuals. This is an apparent reality of late modern life; a milieu characterised by a gradual and systematic loosening of familial and other group bonds. As internet use has become a routine for daily life in late modernity, patrons visit the cyber world as individuals to carry out banking and other purchase transactions. This observation once again, explains the decision to adopt Beck's framework.

- Reflexive agents – individuals are not social dopes in the view of Giddens but reflexive, that is, they are not mere recipients of structure or bounded by structural constraints (Giddens, 1976). Individuals actively shape modernisation by virtue of their actions. This perspective directly challenges the vulnerability thesis which, sought to explain that people simply go along. This observation feeds into the two observations as above, and they together form a chain. The observation here also carries with it important lessons, and a critical niche for the present study. As risks become widespread, and actors increasingly individual, reflexivism becomes a defining distinction among actors. In the context of the threat or risk of cybercrime (credit/debit card fraud) victimisation, agent reflexivism is particularly crucial. Agent reflexivism may include, but not limited to, the adoption of safety standards (behaviour modifications) by users of the computer, especially while online. Seen in this way, the choice to utilise Beck's framework, in an attempt at understanding the determinants of the fear of cybercrime victimisation, becomes clearly underscored.

A final general observation from the works of Beck, Luhmann and Giddens is the apparent lack or absence of the trade-off between benefit and danger which seem to have

been built into their work. In other words, a sense of the benefits arising from new stuff (technology) is missing. People experience and deal with risk and danger, but they also deal with the benefits created as a result by utilising new technological solutions available to them. For example, why do I bank online? Most probably I do so because it is quick, easy and convenient. Combined with the fact people are ensnared on-line anyways, those benefits are enough to offset possible fears/dread that arises from the possibility of being a victim of cybercrime. This observation is significant and may be deemed a common limitation stemming from the work of the three theorists.

As a conclusion to my reflection of Beck's theoretical framework of the Risk society, it is imperative to restate that the lessons revealed in the reflections together form the strong foundation for my choice of theoretical framework. The lessons as seen from the above include the existential realism of risks, individualism and agent or actor reflexivism. To understand the risk of cybercrime (credit/debit card fraud) victimisation therefore, it is imperative to speak directly with students (agents). The reasoning behind this is the fact the risk society framework gives much significance to individuals as agents and actors. This is therefore influencing my choice of methodology, which is the survey (methodology) of students.

3.6. Chapter Summary

The foregoing discussion in this chapter has been focussed on the theoretical literature review, and eventually the theoretical framework adopted for this thesis. The chapter began by examining some previous socio-criminological theories and their attempts at explaining the problem of fear of crime. The vulnerability thesis, the instrumental thesis, the incivilities thesis and psychological factors have been reviewed here. The rationale for the review was to gauge the extent of applicability of those theories to the fear of credit/debit card fraud

victimisation. The thesis argue that all four socio-criminological theories constitute first of all general propositions at explaining broad based ‘ordinary’ street crime, and secondly, they all almost used global measures and do not focus on specific crimes. Following this, a detailed discussion of Beck’s theory of the Risk Society followed, with an examination of some criticisms against Beck’s theory. The chapter also reviewed works of two contemporary sociologists on risk – Luhmann and Giddens – pointing out similarities and differences between their work and Beck’s theory. The chapter concludes with a general reflection from Beck’s theoretical framework of Risk society and with further justifications of why Beck’s theory of Risk Society is the best fit for the thesis.

CHAPTER 4

METHODOLOGY

4.1. Introduction

This chapter presents a detailed discussion of the methodological type, steps and tools used for the study. It also presents information on the variables as well as hypothesis and research questions. All these steps discussed here have been important in arriving at an understanding of the research problem. The research problem underpinning this study is what explains the fear of credit/debit card fraud victimisation among students?

The rest of the chapter proceed by first examining the research design, justification for choice of students and then the tools and instruments. The variables for the study (dependent and independent) together with recoded variables and the rational for each are presented. The sampling framework is also presented with a detailed discussion of the statistical model. The analytical model formulation and link function are also examined under this chapter.

4.2. Research Design

The research utilises the survey methodology to collect data from the University of Saskatchewan, in which students are the unit of analysis. As a popular research tool in criminological research (Yang & Wyckoff, 2010), the survey methodology gathers primary, explorative and important descriptive data from the target population. The data gathered from this approach is quantitative and the themes were derived from a review of the relevant literature as well as from a review of the Saskatchewan Crime study dataset. Subsequently, the survey questions were formulated based on the themes arising from the empirical literature on the field, the Saskatchewan Crime study and my theoretical framework. Using the survey questionnaire also enabled me test relationships between the variables of interest (Creswell, 2009; Bryman, Bell & Teevan, 2012).

The survey methodology was chosen over other methods on the basis of three main factors. First of all, as already mentioned, the study is an exploratory one and survey methodology is reputed as an effective strategy for gathering exploratory data (Yang et al., 2010). Second, given the vastness of the population of interest, the survey methodology offered prudence in terms of reaching out to a significant proportion of the target population. The University of Saskatchewan (2015) estimates the student population to be approximately 20, 998 in the 2015/2016 school year. Given time constraint, a survey was an effective way of reaching the target population. Third, the survey methodology is the method of choice in criminological and especially, fear of crime studies (Yang et al., 2010).

Given the nature of the study, in an ideal world situation, the approach would have been reaching out to all the individual students in the University of Saskatchewan. However, with the constraints of time and material resources in the realistic world, the survey methodology and specifically the voluntary online survey offers the best option for collecting descriptive information comparable with large scale studies.

4.3. Justification for Choice of Students

University students were selected for this research because digital literacy among them has become an important part of their daily routine (Prensky, 2001). As a result, students represent potential victims of cybercrime (credit/debit card fraud). Significantly, the choice of students is consistent with my theoretical framework, which holds that to get an understanding of the risk or threat of victimisation, it is imperative to find out directly from individuals who are seen as reflexive agents. This approach, following on from the theoretical framework is expected to provide much needed breadth (quantitative information) to the problem of fear of cybercrime (credit/debit card fraud) victimisation among students. Even though the suitability of generalising findings from student samples to the wider population remain contentious (Holtfreter, Reisig, Leeper Piquero & Piquero, 2010; Payne &

Chappell, 2008), the choice of a student sample is advantageous in the sense that it helps to leverage the effect that the education variable may have brought into the analysis by providing for homogeneity of educational backgrounds (Yang et al., 2010).

4.4. Tools/Survey Instrument

Tools and equipment for the research was a set of structured survey questionnaires administered online. The survey was developed and hosted on the Qualtrics platform. Qualtrics is an online survey management software and is hosted by the Social Sciences Research Laboratories of the University of Saskatchewan. The draft survey instrument (questionnaire) was pre-tested with a select group of (30) university students and subsequently modified based on comments from participants. Respondents for the pre-testing were randomly selected students across campus. Some of the modifications resulting from the pretesting included expanding the range of options for some multiple choice questions, such as online safety mechanisms employed by students whilst online. Data analysis is done using the Statistical Package Social for the Sciences (SPSS) version 19.

4.5. Ethical Considerations

Every research activity comes with it various ethical issues. This thesis was no different and raised considerable ethical issues. The ethical issues involved embodied the three complementary and mutually reinforcing core principles of respect for persons, concern for welfare and justice (Bryman et al., 2012). The specific ethical issues that arose from this project ranged from informed consent to confidentiality.

In the first place there was the question of convincing participants to participate and to have the confidence no negative consequences arise from their participation. This is the notion of informed consent and it involves subjects giving free, informed and ongoing consent to participate in the study (Bryman et al., 2012:194). This usually arises with highly sensitive phenomenon, however, I did not envisage much difficulty given the ‘less sensitive’

nature of the questions. Participants were informed via e-mail through their PAWS accounts and a general advertisement on PAWS. I took the additional step of going to various lecture halls for a brief announcement before the class begin. The idea was that an increased publicity would result in a higher possibility of an enhanced response rate as well as prompt response time.

Addressing the challenge of informed consent and getting participants to participate in this exercise involved using critical gate keepers. Without doing so it would not be possible to reach the desired participants. A critical gatekeeper for this survey was the university intranet (PAWS announcement platform). Additionally, it was mandatory that participants signed consent forms. The consent involved was implied by completion of the survey. This is because before being allowed to complete the survey, students were required to agree to the consent information. Failure to accept the consent information meant that students were not allowed to complete the survey. In addition, the consent form had the researchers' contact information, where they could address concerns they had before agreeing to the terms. As well, my role as an insider (a student and a teaching assistant) was also useful in complementing the gate keeper role. As the student researcher, I also spoke with the students to the effect that the exercise was purely academic and that no specific identifiers would be captured in the information provided. Critically participants were made aware that participation is strictly voluntary, even though I very much craved their assistance.

Related to the challenge of informed consent is confidentiality. Within the dataset, each student was given a unique identification (ID) number and the information that they provide in the survey is associated with the ID number. The implication of the online approach was that there was no chance for the researcher to attach names to faces. Importantly the survey did not request names and other identifiable information of respondents.

4.6. Reflectivity

The choice of the thesis topic was influenced by a number of factors, but mainly personal experiences and academic interest. My background as a student from the global south was very crucial in this. I have been fortunate to have had the opportunity to travel around the world and to interact with youth from both worlds (the global north and south). Through this I have been able to gain an idea of the relative opportunities and challenges facing youth from the different worlds. As a third world student from a low to middle class family, I observed a lot of my cohorts and even much younger ones, who facing similar problems like myself and others, resorting to different routes in life. These youth have mostly and consistently referred to the educational paths taken by myself and others, as a long and mostly unproductive one. They readily point to several unemployed but brilliant young graduates straddling the streets without opportunities for gainful employment. Sadly a significant number of these youth therefore spend much productive hours at internet cafes practising various forms of internet fraud. This is while their colleagues in the developed world mostly spend similar time exploring the internet for educational and other beneficial ends. This brief background to a very large extent has informed my decision to explore the chosen topic.

Consequently my goals in pursuing this project are first of all to understand as close as possible, the incidence of the risk or fear of cybercrime among students. I am also hoping to be able to establish whether there is a gendered fear among these students. Another goal is to assess students understanding of cybercrime to see if it is consistent with variations of definitions in the literature. Invariably my goal is to be able to situate this phenomenon theoretically within a sociological lens, that is, the risk theory of Beck. This approach is seen as a way to provide a much nuanced understanding of the fear of crime.

4.7. Hypotheses

To understand the problem and to arrive at answers to the research questions, this study was guided by four main hypotheses. The hypotheses tested in the study included;

Hypothesis 1: Students who believe cybercrime is both cyber-enabled and cyber-dependent are less fearful than students who believe cybercrime is either cyber-enabled or cyber-dependent.

To test the hypothesis that students' knowledge of cybercrime influences their fear of credit/debit card fraud, the appropriate null and alternate hypotheses are;

Null Hypothesis (H_0): There is no significant difference in student's fear of credit/debit card fraud, irrespective of their knowledge of cybercrime.

Alternate Hypothesis (H_1): Students who believe cybercrime is both cyber-enabled and cyber-dependent are less fearful of credit/debit card fraud, compared to students' who believe cybercrime is either cyber-enabled or cyber-dependent.

The independent variable for this hypothesis is Knowledge of Cybercrime (Q1 see Appendix A), while the dependent variable is Fear of Credit/Debit card fraud victimisation.

Hypothesis 2: Socio-demographic factors significantly affect fear of credit/debit card fraud victimisation (females, older people, single, non-whites with higher income are expected to be more fearful of credit/debit card fraud victimisation).

To test the hypothesis that students' socio-demographic factors will significantly affect their fear of credit/debit card fraud, the appropriate null and alternate hypothesis are;

Null hypothesis (H_0): Student's socio-demographic factors will produce no significant difference in their fear of credit/debit card fraud (females, older students, single, non-whites with higher income have no more significant fear compared to males, younger, non-single, white students with less income).

Alternate Hypothesis (H_1): Socio-demographic factors will produce a significant difference in students' fear of credit/debit card fraud (females, older, single, non-white students with higher income will express significantly more fear).

The independent variable here again is Fear of Credit/Debit card fraud victimisation. The dependent variable on the other hand includes all the socio-demographic variables (gender, age, marital status, ethnicity, income; see questions 22 through to question 31 from the questionnaire in Appendix A).

Hypothesis 3: Internet use behaviours affect students' risk of credit/debit card fraud victimisation.

To test the hypothesis that students' internet use behaviours affect their risk of cybercrime (credit/debit card fraud) victimisation, the appropriate null and alternate hypothesis are;

Null Hypothesis (H_0): Internet use behaviours will produce no significant difference in students' risk of credit/debit card fraud victimisation.

Alternate Hypothesis (H_1): Internet use behaviours will significantly increase students' risk of credit/debit card fraud victimisation.

The dependent variable for this hypothesis is Feeling of risk (question 4) and the independent variables include questions 13 through to question 19 (place of regular internet access – Q13, medium of internet access – Q14, frequency of internet use – Q15, time spent on the internet – Q16, online purchase – Q17, frequency of online purchase – Q18 and online safety precautions – Q19, see questionnaire in Appendix A). However, only question numbers 13, 15, 16 and 17 have been tested using binary logistic regression. The remaining questions (Q14, Q18 and Q19) have been examined using crosstabs (chi-square). The reason is that the latter sets of questions are all multiple response questions, the reason for which they were not suitable for binary logistic regression.

Hypothesis 4: Past victims of credit/debit card fraud are more fearful of credit/debit card fraud victimisation.

To test the hypothesis that students with prior experience of victimisation will tend to significantly have more fear of credit/debit card fraud compared to students without experience, the appropriate null and alternate hypothesis are

Null Hypothesis (H_0): experience of victimisation will produce no significant difference in fear of credit/debit card fraud between students with experience and those without experience.

Alternate Hypothesis (H_1): Students with prior experience of victimisation will have significantly more fear of credit/debit card fraud compared to students without experience of victimisation.

The dependent variable for this hypothesis, like in hypotheses 1 and 2 previously, is Fear of Credit/Debit card fraud victimisation. The independent variable on the other hand is Credit/Debit card fraud victimisation, a variable derived from question number 9, which asks: “Did anyone steal your credit/debit card or use your card information to obtain credit in the past twelve months (see questionnaire in Appendix A).

4.8. Variables

Like all quantitative research projects, the research has two main streams of variables, that is, dependent and independent variables.

The variables and responses were both coded automatically via the survey management program (Qualtrics) and SPSS. Initial coding of the questions were done on Qualtrics by identifying each question with a specific question number and under specific question blocks. Responses were coded automatically to correspond with the question numbers in the survey. It is important to add here that the survey questions were made to align with key variables derived from the literature. Subsequent variable recoding and data

analysis were both executed using SPSS. Missing data were treated as missing completely at random, for which reason they haven't been excluded.

The choice of outcome (dependent) variables here are significant because they would contribute to answering my research questions and ultimately my research problem. Significantly, the outcome variables are a direct reflection of my theoretical framework. Also instead of a single outcome variable, the two outcome variables employed in this study are necessary because they each answer specific questions. As a result, employing them in this way is envisaged to lead to a comprehensive finding in respect of my research questions and my research problem.

On the other hand, the independent variables for the study are a direct reflection of the literature on the field. The literature specifically identifies four variables (socio-demographic factors, knowledge of cybercrime, internet use behaviours and victimization experiences) to explain crime victimisations (Anderson, 2006; Callanan et al., 2015; Hale, 1996; Roberts et al., 2013 etc.). In referring to these, the literature relates the variables more consistently with 'conventional' crimes. In this regard, the idea is also to establish to what extent these variables apply to cybercrimes and specifically, credit/debit card fraud (see Appendix A for complete list of questions and measurements).

4.8.1. Dependent Variables:

The dependent variables in the study are twofold, thus;

1. Fear of Credit/Debit card fraud victimisation – this was measured in the study by the question: During the past month, have you ever felt fearful about being the victim of credit/debit card fraud? Response categories were “Yes” and “No”.
2. Risk of Credit/Debit card fraud victimisation – the relevant question in the study was: Compared to other crimes (physical crimes), do you feel more at risk of Credit/Debit Card fraud? Response categories include “Yes” and “No”.

4.8.2. Independent Variables:

The research involved a number of independent variables based on those identified in the literature (see Appendix A for complete list of questions and measurements). These include;

1. Socio-demographic factors – gender, age, marital status, ethnicity, family income, residence status, employment. These variables were measured by the questions

Gender - Please indicate your gender? (Male, Female, Other, Prefer not to say)

Age - Please indicate your age range... (Under 17 years, 17-23 years, 24-30 years, 31-37 years, 38-44 years, 45-51 years, 52 years and over)

Marital Status - Please indicate your current marital status? (Single (Never legally married), Legally married (and not separated), Separated, but still legally married, Living with a common-law partner, Divorced, Widowed)

Ethnicity - What ethnicity do you identify with? (Aboriginal, White/Caucasian, African, Asian, Other (please specify)...)

Residence Status - What is your Residency status? (Domestic Student (citizen or permanent resident), International Student)

Employment/work status - What best describes your current employment status?
(Working part time, Working Full time, Not working)

Family income - What category best describes your annual total family income, from all sources before taxes?
2. Knowledge/perception of cybercrime – this was measured by the question: In your view, what constitutes cybercrime? Responses included “Crimes committed using computer or its systems as the tool (cyber-enabled)”, “Crimes committed using computer or its systems as the target (cyber-dependent)”, and “All of the above”
3. Internet use behaviour - internet use behaviour is measured in terms of

- i. Place of internet access - Where do you mostly access internet from?
 - ii. Media of internet access - How do you access the internet? (please select all that apply)
 - iii. Frequency of internet use/access - How frequently do you use the internet?
 - iv. Average time spent on the internet at any one time - On average, how much time do you spend on the internet each time you go online?
 - v. Online purchase - During the past 12 months, have you used the internet to purchase anything online?
 - vi. Frequency of online purchase - About how many times a month did you purchase something online, during the past year?
 - vii. Internet use safety precautions - What specific safety precautions do you employ while using the internet – to shop online or to access sensitive information?(choose all that apply)
4. Experience of victimisation – this was measured by the question: During the past 12 months, did anyone steal your credit/debit card or use your card information, without your permission to obtain money or credit? “Yes” and “No”

4.8.3. Recoded Variables

Some of the variables were recoded for clarity and organisation. The variables recoded include;

- i. Place of Residence – the original place of residence variable included University residence, Off-campus Urban and Off-campus Rural. The newly recoded place of residence variable is University residence and Off-campus residence.

I decided to merge the off campus-urban and off-campus rural categories because the frequency for the off-campus rural was too small (5.5 per cent) and would not add statistical value to the analysis. In addition, the characteristics of the two merged

categories were very similar on all the key indicators examined in the study. By merging the categories we have a better distribution of the residence variable (on-campus 24.6 per cent and off campus 75.4 per cent).

- ii. Level of studies – the original level of studies variable included Undergraduate 1st, 2nd, 3rd, 4th or more, Graduate 1st, 2nd, 3rd, 4th or more and Other (specify). The newly recoded level of studies variable is now Undergraduate, Graduate and other (specify). These categories were created because the frequencies for the original variables were too small for meaningful analysis. In addition, the graduate/undergraduate dichotomy is a more established way of studying student populations (see Alshalan, 2006; Yu, 2014). My recoded categories are therefore more reliable and comparable to other studies.

- iii. Age categories – the original age categories included Under 17 years, 17-23 years, 24-30 years, 31-37 years, 38-44 years and 45-51 years.

The recoded age categories are now 23 years or less, 24-37 years, 38-51 years or more.

This variable was recoded to reduce the categories because the frequencies in some of the original variables were too small and would not allow for meaningful analysis [for example under 17 years (0.7%), 38-44 years (3%), 45-51 years (0.5%)]. In addition, the three recoded categories more clearly reflect stages of the life cycle (young adulthood, middle adulthood and mature adults). A similar classification has also been used in related studies (see Braungart et al., 1980). This allowed me to speak to how fear/cybercrimes affect the different demographics differently.

- iv. Annual family income – the original annual family income variable included Less than \$25,000, \$25,000 to less than \$50,000, \$50,000 to less than \$75,000, \$75,000 to less than \$100,000, \$100,000 to less than \$125,000, \$125,000 or more.

The newly recoded annual family income variable includes \$49000 or less, \$50000 to less than \$100000 and \$100000 or more.

This variable was recoded to allow for comparability with other studies. The new categories crudely reflect stratification: low income, middle income and high incomes. This classification is also used in similar research (see Anderson, 2006) hence this increases the reliability and comparability of my research.

- v. Marital Status – the original marital status variable included Single (Never legally married), Legally married (and not separated), Separated, but still legally married, Living with a common-law partner, Divorced and Widowed. Categories for the newly recoded marital status variable include Single and Married.

Similar to the original age variable, this variable was recoded to reduce the categories because the frequencies in the original variable were too small and would not allow for meaningful analysis [for example legally married (and not separated) (6.2%), separated but still legally married (0.2%), living with a common law partner (6.4%), divorced (1.2%)]. Additionally, the two recoded categories reflect more clearly and closely the marital status of respondents (given the sample is from a student population). It also reflects the broader perspective of marital status (the single verses married dichotomy), and hence enabled me uncover and to speak to how fear and risk affect the married as well as single students differently. More over this classification has been used in similar studies (see Parker, 1988).

- vi. Study Mode – the original study mode variable included Full time, Part time and Not applicable. The newly recoded study mode variable has categories Full time and Part time. The recoding of this variable is deemed necessary because the previous category, which included not applicable, does not make much analytical sense within

the context. Given that the sample included only students, the appropriate category is either full time study or part time study.

4.9. Sampling

The population universe for the research is the students of University of Saskatchewan and the sampling frame includes all the students of the university. The study used a convenience sample (non-probability sampling) using the survey questionnaire on an online interface. As a result, instead of the researcher selecting respondents, there was a self-selection by students (respondents) themselves. Consequently the decision to participate was made by individual students. To excite much interest and to increase the chances of sample representation with the given population, the researcher made efforts to advertise the study through various campus media. However, since respondents selected themselves, it was not feasible to employ the equal probability of selection method as advocated for in probability sampling. The equal probability of selection method is a fundamental principle of probability sampling (Healey, 2009).

With the online framework, the survey became available to all students of the University of Saskatchewan. Hosting the survey online also afforded students an equal probability of participation, albeit by self-selection. The study was also advertised and re-advertised on PAWS (the university's intranet, which is available to students). Recruitment posters were also placed at vantage points on the university campus. The online nature of the survey made it possible for students to complete the survey as individuals and at their own convenient times and places. However, the researcher acknowledges the possibility of selection bias, in that respondents were not individually selected. As a result, who is most likely to participate or to not participate in an online survey remain an issue. Having said this, the sampling approach adopted in this study is still valid given the focus of the research. Who

utilizes the internet and when they choose to use it are both dependent on an individual's needs and motivations at any given point in time.

From a student population of 20, 998 based on statistics from the fall of 2015 (University of Saskatchewan, 2015), a sample size of 377 was needed as the minimum for significant representation of the entire student population using the sample size calculator at the 95% confidence interval (Creative Research Systems, 2012). At the end, a total of 464 students participated in the study, with 405 completing the entire survey.

4.10. Analytical Models

The data were placed in frequency tables to show aggregates in respect to particular variables as well as to represent responses to key questions. In addition, comparative charts and bivariate tables were used to show relationships between variables such as gender and fear of credit/debit card fraud victimisation as well age and fear of credit/debit card fraud victimisation among others. To predict outcomes, I employed binary logistic regression. In order to determine statistical significance, the p-value was used to evaluate whether the assumed (null) hypothesis is true. The null hypothesis for all statistical tests was that there is no significant association between the independent and dependent variables. A p-value of less than 0.05 indicates that there are significant relationship between the independent and dependent variables.

Logistic regression is part of a category of statistical models called generalized linear models. This broad class of models includes ordinary regression and ANOVA, as well as multivariate statistics such as ANCOVA and loglinear regression (McCullagh & Nelder, 1989). Logistic regression allows one to predict a discrete outcome, such as group membership, from a set of variables that may be continuous, discrete, dichotomous, or a mix of any of these (Agresti, 1990). In simple terms Logistic regression is useful for predicting a binary dependent variable as a function of predictor variables. The goal of logistic regression

is to identify the best fitting model that describes the relationship between a binary dependent variable and a set of independent or explanatory variables (McCullagh et al., 1989).

The linear logistic model assumes a dichotomous dependent variable Y with probability π , where for the i th case,

$$\pi_i = \frac{\exp(\eta_i)}{1 + \exp(\eta_i)} \text{ (Equation 4.01)}$$

Or

$$\ln\left(\frac{\pi_i}{1 - \pi_i}\right) = \eta_i = \mathbf{X}'_i \boldsymbol{\beta} \text{ (Equation 4.02)}$$

Where $\eta_i = \mathbf{X}'_i \boldsymbol{\beta} = \beta_0 + \beta_1 X_{i1} + \dots + \beta_k X_{ik}$ (Equation 4.03); the β 's are the model parameters and X_i 's are the explanatory variables.

4.10.1. Generalised Linear Models (GLM)

Generalized linear models (GLM) were first introduced by Nelder and Wedderburn (Agresti, 1990). They provided a unified framework to study various regression models, rather than a separate study for each individual regression. It includes linear regression models, analysis of variance models, logistic regression models, Poisson regression models, log-linear models, as well as many other models (McCullagh et al., 1989). The above models share a number of unique properties, such as linearity and a common method for parameter estimation. According to Agresti (1990: 80), a generalized linear model consists of three components:

1. A *random component*, specifying the conditional distribution of the response variable, Y_i given the explanatory variables.
2. A linear function of the regressors, called the *linear predictor*,

$\eta_i = \alpha + \beta_1 X_{i1} + \dots + \beta_k X_{ik} = \mathbf{x}'_i \boldsymbol{\beta}$ (Equation 4.04) on which the expected value μ_i of Y_i depends.

3. An invertible *link function*, $g(\mu_i) = \eta_i$ (Equation 4.05) which transforms the expectation of the response to the linear predictor. The inverse of the link function is sometimes called the *mean function*: $g^{-1}(\eta_i) = \mu_i$ (Equation 4.06).

4.10.2. Model Formulation

It is important to understand that the goal of an analysis using logistic regression is the same as that of any model-building technique used in statistics: To find the best fit and most parsimonious (McCullagh, 1989). What distinguishes a logistic regression model from linear regression model is the outcome variable. In the logistic regression model, the outcome variable is binary or dichotomous (McCullagh, 1989).

Logistic regressions work with **odds** rather than proportions (McCullagh, 1989). The odds are simply the ratio of the proportions for the two possible outcomes. If \hat{p} is the proportion for one outcome, then $1 - \hat{p}$ is the proportion for the second outcome:

$$ODDS = \frac{\hat{p}}{1 - \hat{p}} \text{ (Equation 4.07)}$$

A similar formula for the population odds is obtained by substituting π for \hat{P} in this expression.

To use categorical variables in logistic regression as we have in this study, we need to use a numeric code. The usual way to do this is with an indicator variable. For our purpose we used an indicator of whether or not a respondent has ever felt fearful about being the victim of credit/debit card fraud:

$$y = \begin{cases} 1, & \text{If the respondent has ever felt fearful} \\ 0, & \text{If the respondent has never felt fearful} \end{cases} \text{ (Equation 4.08)}$$

In simple linear regression we model the mean μ of the response variable y as a linear function of the explanatory variable: $\mu = \beta_0 + \beta_1 X$ (Equation 4.09). With logistic regression we are interested in modelling the mean of the response variable π in terms of an explanatory variable x . We could try to relate π and x through the equation

$\pi = \beta_0 + \beta_1 X$ (Equation 4.10). Unfortunately, this is not a good model. As long as $\beta_1 \neq 0$, extreme values of x will give values of $\beta_0 + \beta_1 X$ that are inconsistent with the fact that $0 \leq \pi \leq 1$ (McCullagh, 1989).

The logistic regression solution to this difficulty is to transform the odds ($\pi/(1 - \pi)$) (Equation 4.11) using the natural logarithm. We use the term **log odds** for this transformation (McCullagh, 1989). We model the log odds as a linear function of the explanatory variable:

$$\log\left(\frac{\pi}{1 - \pi}\right) = \beta_0 + \beta_1 X \text{ (Equation 4.12)}$$

4.10.3. The Link Function

In theory, link functions $\eta_i = g(\mu_i)$ (Equation 4.13) can be any monotonic, differentiable function (McCullagh, 1989). In practice, only a small set of link functions are actually utilized. In particular, links are chosen such that the *inverse link* $\mu_i = g^{-1}(\eta_i)$ (Equation 4.14) is easily computed, and so that g^{-1} maps from $X_i\beta = \eta_i \in \{ \}$ (Equation 4.15) into the set of admissible values for μ_i . A logit link is usually used for the Logistic regression model, since $\mu_i = g(\mu_i) \in \{ \}$ (Equation 4.16), and because Y_i is dichotomous (McCullagh, 1989).

Examples of link functions that are used are the identity, log, inverse, logit, probit, log-log, complementary log – log among others (Agresti, 1990).

Following a description of the modelling and link function, results of the modelling (binary logistic) will be reported using odds and probabilities. The odds ratios will be reported first, and then subsequently converted into odds. The implication of the results in terms of probabilities will finally be reported.

4.11. Chapter Summary

This chapter provides details of the methods employed for this research work. It began by identifying the survey methodology as the method of choice for most

criminological studies. Consequently, the survey methodology has been employed for the study. The survey methodology is conceived as a tool effective at gathering primary, explorative and important descriptive data from the target population. Students constitute the target population and the choice is justified by the fact of their positioning in the contemporary (techno-scientific) era. By virtue of their status as students and constituting the critical majority youth, internet use remains an important part of their daily routine. The survey instrument is identified as a set of structured questionnaire, developed and hosted online through Qualtrics. Variables for the study are identified with a further provision of the variables that were recoded with an explanation of the rationale in each case. This is followed by a description of the sampling framework. Finally, the statistical model is presented in detail, with a description of both the model formulation and link function.

CHPATER 5

FINDINGS

5.0. Introduction

This chapter presents descriptive statistics to reveal relationships between key socio-demographic and other variables and the dependent variables in the study. The chapter further presents results of the findings from the various statistical tests in respect of hypotheses.

Results of binary logistic regression and bivariate tests will be presented. The tests cover all four hypotheses, which are in themselves linked to the research questions.

5.1. Descriptives

5.1.0. Socio-demographic factors and fear of Credit/Debit card fraud victimisation

5.1.1. Gender and Fear of Credit/Debit card fraud

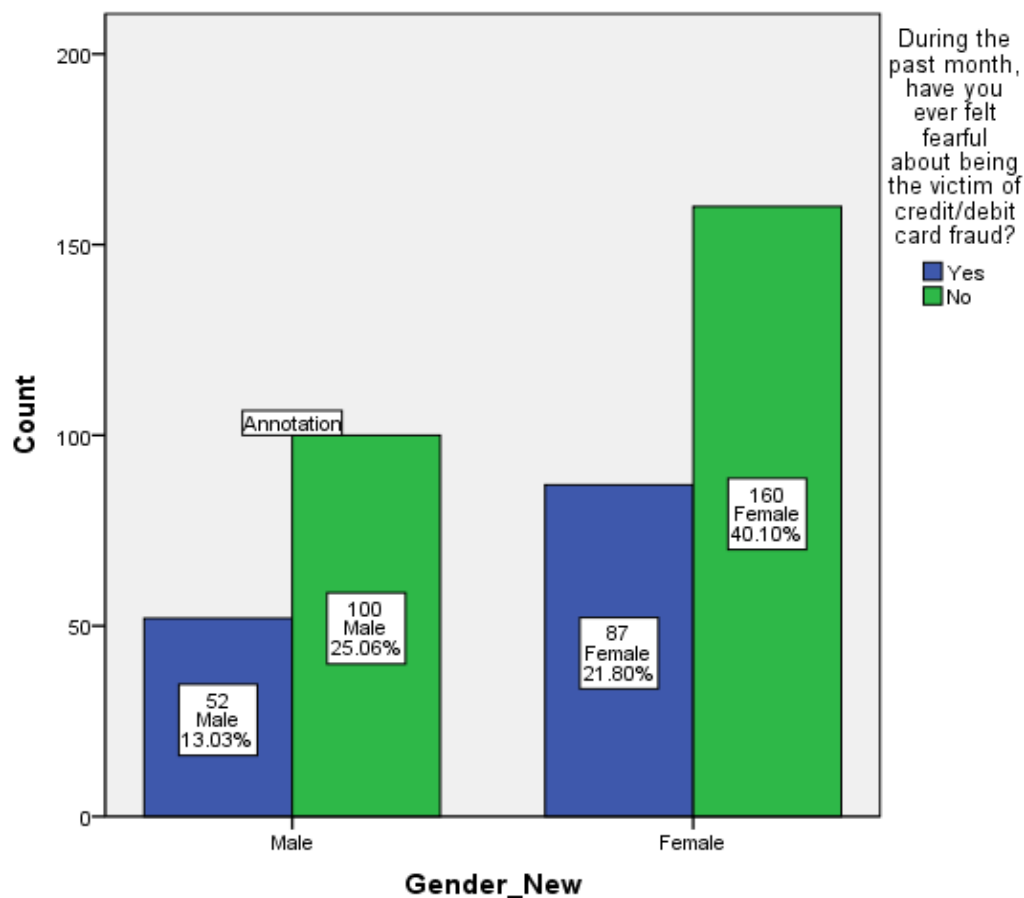


Figure 5.01. Relationship between Gender and Fear of Credit/Debit card fraud

Figure 5.01 indicates the relationship between gender of students and fear of credit/debit card fraud victimisation. The graph reveals that female students experience higher feelings of vulnerability and hence fear of credit/debit card fraud, almost doubling the vulnerability expressed by male students (about 22 percent or 87 students). For male students on the other hand, only 52 students (13.03 percent) report feeling vulnerable. The graph therefore reveals some form of relationship between gender and fear of credit/debit card fraud victimisation.

5.1.2. Full time/Part time study and Fear of Credit/Debit card fraud

Figure 5.02 shows the relationship between study mode (full or part time) and fear of credit/debit card fraud victimisation. Full time students experience very little fear (61.5 percent) as well as an appreciable amount of fear (33.9 percent). Part time students also tend to experience very little to almost no fear. The difference within part time students is also almost non-noticeable, with 1.7 percent expressing fear and 2.7 percent having no fear. In all instances, the graph indicates that studentship status (full or part time) does not produce much aggregate difference in terms of fear among students.

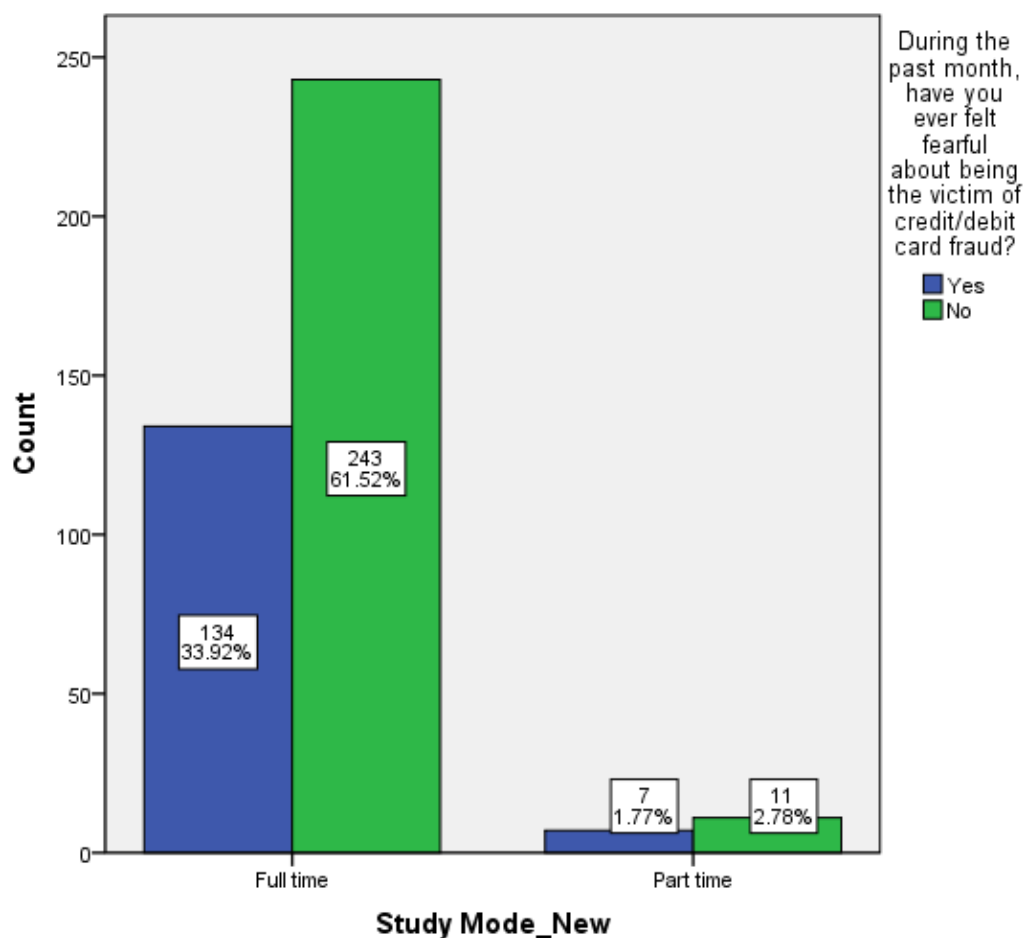


Figure 5.02. Relationship between Study mode and Fear of Credit/Debit card fraud

5.1.3. Residency Status and Fear of Credit/Debit card fraud

Figure 5.03 is a graph showing the relationship between residency status and students fear of credit/debit card fraud victimisation. The graph reveals a much pronounced fear of credit/debit card fraud among domestic students (27.79 percent) compared to international students (7.44 percent). However in absolute terms, fear is much less among domestic students (56.44 percent compared with 27.72 percent). On the other hand even though fear is less pronounced among international students too, the difference among international students is just by one unit (7.43 percent and 8.42 percent).

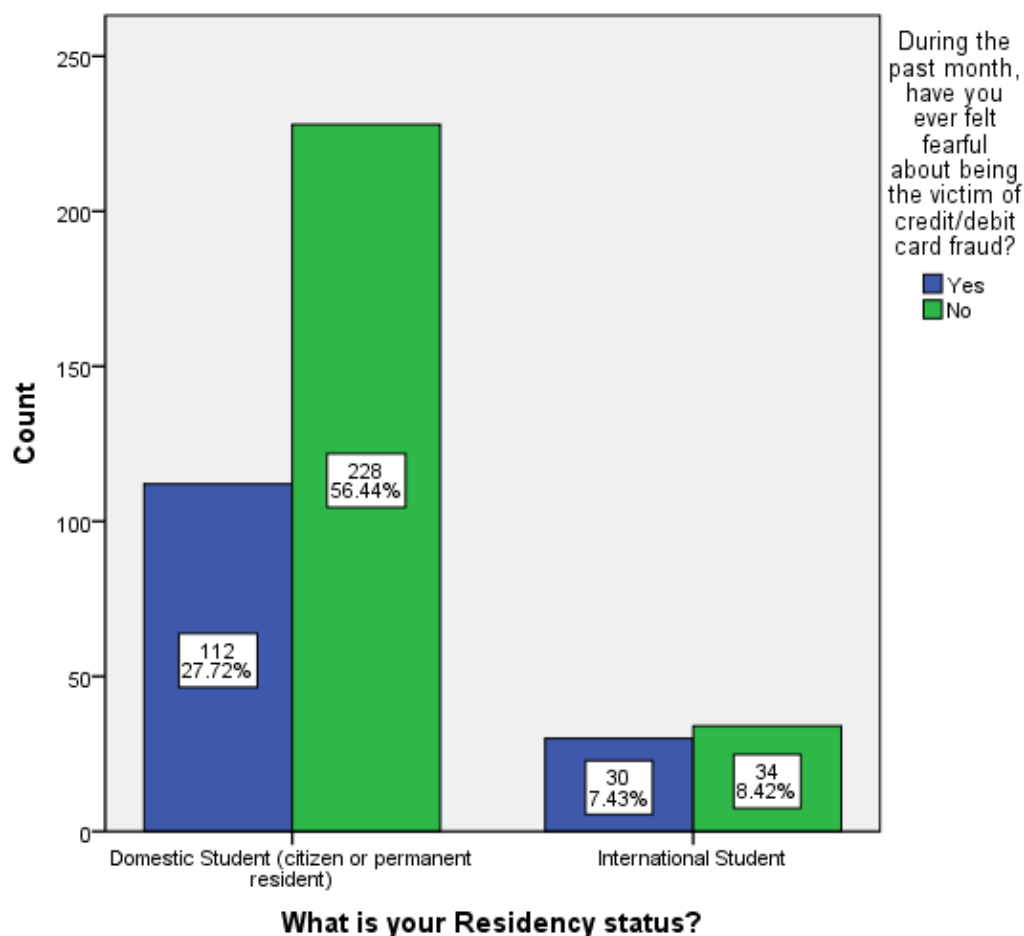


Figure 5.03. Relationship between Study mode and Fear of Credit/Debit card fraud

5.1.4. Place of residence and Fear of Credit/Debit card fraud

Figure 5.04 demonstrates the relationship between students' place of residence and fear of credit/debit card fraud victimisation. The figure reveals that fear is more pronounced among off-campus residence students compared to university residence students. Specifically, 26.8 percent (108) of off-campus residence students express fear compared with 8.68 percent of university residence students. Equally whereas 48.64 percent of off-campus residence students express no fear, 15.88 percent of students in university residence do not experience fear. However, generally the graph reveals that student's place of residence is negatively related to fear of credit/debit card fraud.

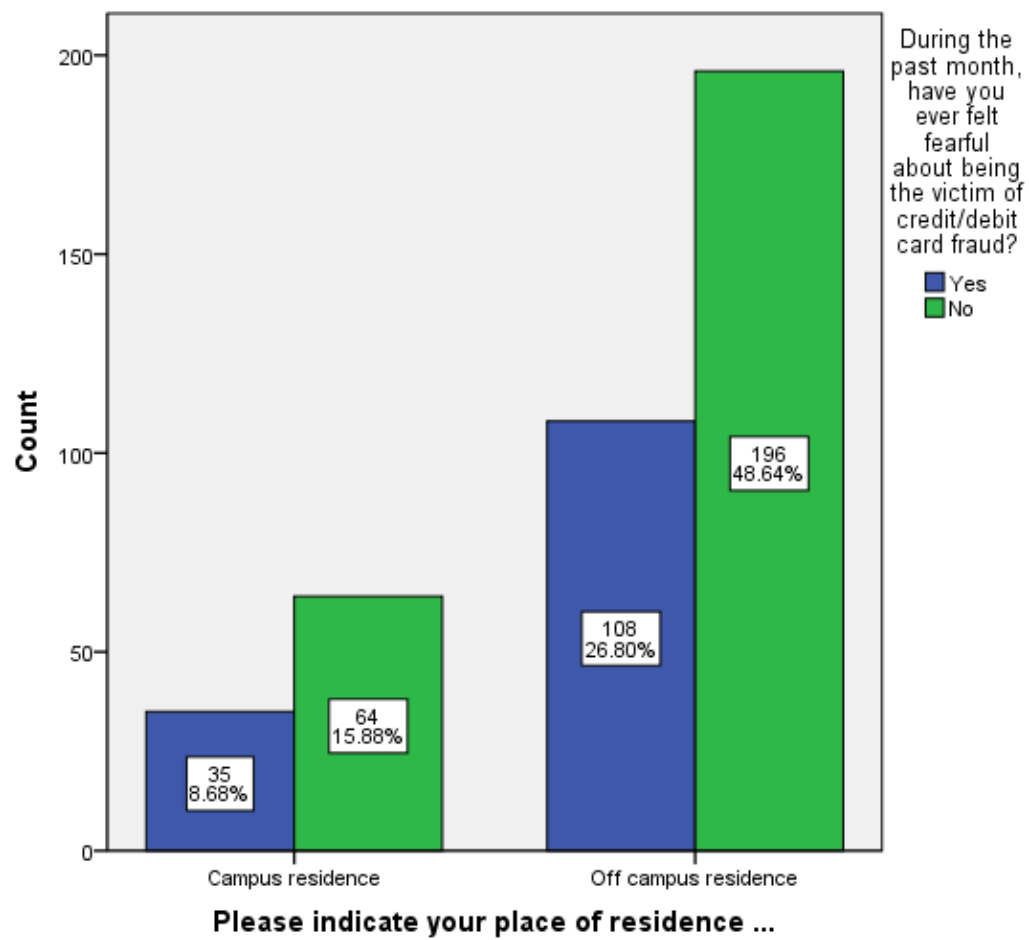


Figure 5.04. Relationship between Place of residence and Fear of Credit/Debit card fraud

5.1.5. Employment/Work status and Fear of Credit/Debit card fraud

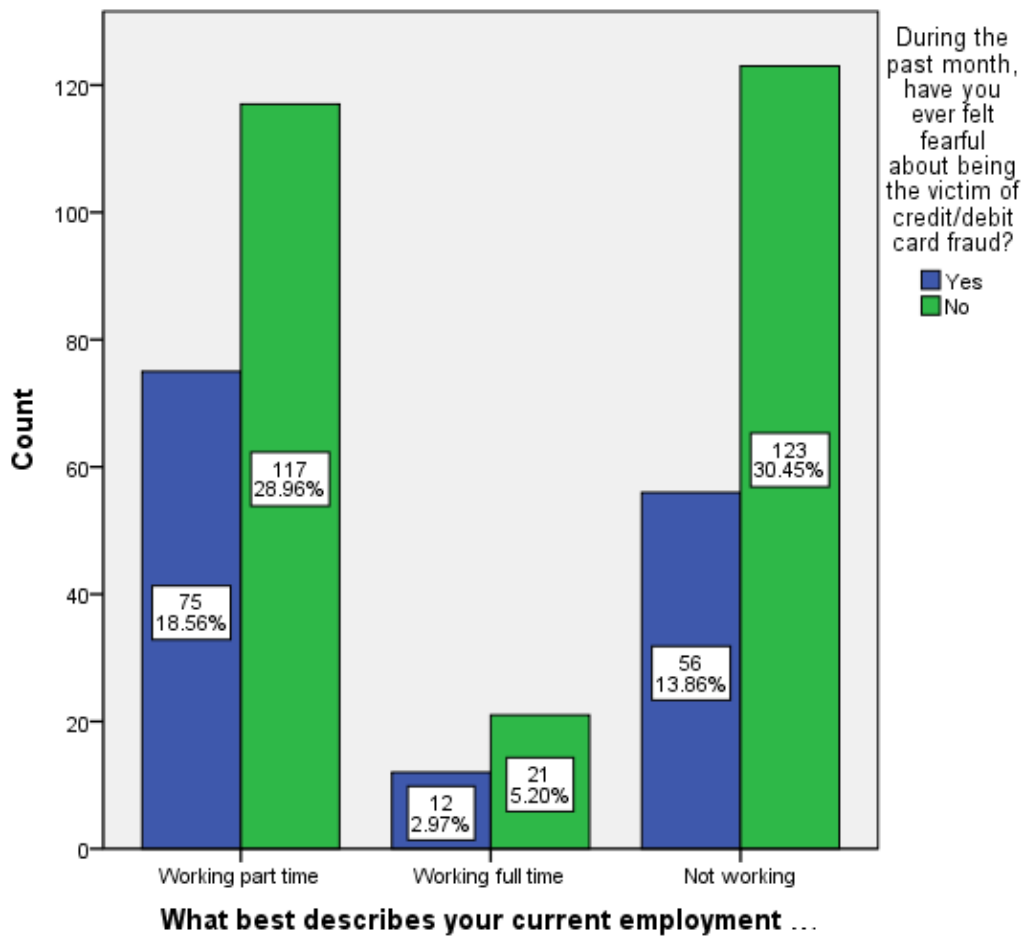


Figure 5.05. Relationship between Current employment/work status and students' Fear of Credit/Debit card fraud

Figure 5.05 presents a histogram of the relationship between student employment status and their fear of credit/debit card fraud victimisation. The graph reveals more instances of fear among students working part time (18.56 percent) and a least amount of fear among students working full time (2.97 percent). However students not working at all report the highest rate of feeling secure (not having fear) in the past month, with full time working students reporting the least (not having fear), that is 5.2 percent compared to the other two groups. The graph also reveals that students working part time and students not working both report similar or identical rates of not experiencing fear (29 percent or 117 students and 30

percent or 123 students respectively). Once again as observed from the graph, fear of credit/debit card fraud victimisation is generally less pronounced among students, irrespective of their employment/work status.

5.1.6. Age and Fear of Credit/Debit card fraud

Table 5.06

Chi-Square Test and Descriptive Statistics for relationship between Age and Fear of Credit/Debit card fraud victimisation

Age Range	During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?	
	Yes	No
23 years or less	93 (33.1%)	188 (66.9%)
24 – 30 years	37 (41.1%)	53 (58.9%)
31 years or older	13 (38.2%)	21 (61.8%)
N = 405		

Notes: $\chi^2 = 2.056$, $df = 2$. The numbers in parentheses indicate column percentages.
 $p > .05$

Table 5.06 reveals that fear is relatively more pronounced among middle age students (24-30 years) with a frequency of 41.1 percent compared to the other age groups. On the other hand younger students (23 years or less) have the least fear (33.1 percent) with (38.2 percent) of elderly students also experiencing fear. The reverse is also true with younger students (23 years or less) reporting the highest rate of feeling secured (66.9 percent) followed by elderly students with 61.8 percent not having fear. Middle age students tend to experience the least amount of not having fear (58.9 percent). Even though generally the table reveal age is not significant, fear is observed to be more prevalent among the advanced student age groups.

5.1.7. Level of Studies and Fear of Credit/Debit card fraud

Table 5.07 shows the relationship between students' level of studies and fear of credit/debit card fraud victimisation. The table reveals that graduate students generally appear to report increased fear compared to undergraduate students and the other category of students (43.7 percent against 33.7 percent and 20 percent respectively). Once again the graph tends to suggest that level of studies is unrelated to students' fear of credit/debit card fraud victimisation.

Table 5.07

Chi-Square Test and Descriptive Statistics for relationship between Level of studies and Fear of Credit/Debit card fraud victimisation

During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?		
Level of Studies	Yes	No
Undergraduate	111 (33.7%)	218 (66.3%)
Graduate	31 (43.7%)	40 (56.3%)
Other	1 (20.0%)	4 (80.0%)
N = 405		

Notes: $\chi^2 = 3.037$, $df = 2$. The numbers in parentheses indicate column percentages.
 $p > .05$

5.1.8. Ethnicity and Fear of Credit/Debit Card fraud

Table 5.08 is the cross tabulation of the relationship between ethnic identity and fear of credit/debit card fraud victimisation. The table reveals that students who identify as Aboriginal report experiencing more fear (42.9 percent), followed by students identifying as Asian (37.5 percent), compared to students who identify with all other ethnicities. Students from 'Other' ethnicities report the least amount of fear (33.3 percent) and closely followed by students who identify as African (34 percent). On the other hand 34.7 percent of Students

identifying as White/Caucasian report having fear. The table also reveals that in all cases, however, fear of credit/debit card fraud among students across all ethnicities is generally low, averaging about 36.8 percent.

Table 5.08

Chi-Square Test and Descriptive Statistics for relationship between Ethnicity and Fear of Credit/Debit card fraud victimisation

Ethnic Identity	During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?	
	Yes	No
Aboriginal	6 (42.9%)	8 (57.1%)
African	17 (34.0%)	33 (66.0%)
Asian	21 (37.5%)	35 (62.5%)
White/Caucasian	90 (34.7%)	169 (65.3%)
Other (please specify)	8 (33.3%)	16 (66.7%)
N = 403		

Notes: $\chi^2 = .581$, $df = 4$. The numbers in parentheses indicate column percentages.
 $p > .05$

5.1.9. Marital Status and Fear of Credit/Debit card fraud

Table 5.09 demonstrates the relationship between marital status and students' fear of credit/debit card fraud victimisation. The table reveals that about one-third each of single (never legally married students) and not single students both express fear (35.1 percent and 38.6 percent respectively). This means less than half of both sets of students have fear of credit/debit card fraud victimisation. Hence, the table suggests marital status is unrelated to students' fear of credit/debit card fraud victimisation.

Table 5.09

Chi-Square Test and Descriptive Statistics for relationship between Marital status and Fear of Credit/Debit card fraud victimisation

During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?		
Marital Status	Yes	No
Single (Never legally married)	121 (35.1%)	224 (64.9%)
Not single	22 (38.6%)	35 (61.4%)
N = 405		

Notes: $\chi^2 = .265$, $df = 1$. The numbers in parentheses indicate column percentages.
 $p > .05$

5.1.10. Income and Fear of Credit/Debit card fraud

Table 5.10 reveal that, fear is generally low among students, across all annual family income categories, averaging about 34 percent. Students in the middle income category (between 50,000 and less than 100,000) have the most fear among the three groups (41.7 percent). On the other hand, students in the higher income category (100,000 or more) have the least fear of victimisation. Low income category of students' are in the middle range, with a fear level of 33 percent. The observation here is that family income is unrelated to fear of credit/debit card fraud victimisation.

Table 5.10

Chi-Square Test and Descriptive Statistics for relationship between Family Income and Fear of Credit/Debit card fraud victimisation

During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?		
Annual total income (\$)	Yes	No
49,000 or less	58 (33.0%)	118 (67.0%)
50,000 and <100,000	30 (41.7%)	42 (58.3%)
100,000 or more	14 (28.6%)	35 (71.4%)
N = 297		

Notes: $\chi^2 = 2.587$, $df = 2$. The numbers in parentheses indicate column percentages.
 $p > .05$

Table 5.11

Frequency distribution of respondents Knowledge of Cybercrime

In your view what constitutes cybercrime?	
Knowledge of Cybercrime	Frequency
Crimes committed using computer or its system as tool (Cyber-enabled)	49 (11.7%)
Crimes committed using computer as the target (Cyber-dependent)	19 (4.5%)
All the above	350 (83.7%)
N = 418	

5.2. Frequency of Knowledge of Cybercrime

Table 5.11 reveals that very few of the respondents believe cybercrime was either cyber-enabled (11.7 percent) or cyber-dependent (4.5 percent). However, an overwhelming majority of students (83.7 percent) or 350 students, believed that cybercrime was both cyber-

enabled and cyber-dependent. In other words, majority of the respondents had what we can call a comprehensive knowledge of cybercrime.

5.3. Frequency of Internet use behaviours

Table 5.12 shows respondents mediums of internet access. The table reveals that majority of the respondents (87.8 percent and 81.5 percent) accessed internet through their laptops and phones. Desktop was used 29.9 percent, with 109 students accessing through their tablet while 2.7 percent (11 students) used other media to access the internet.

Table 5.12

Frequency distribution of Medium of Internet access by respondents

Medium of Internet access ^a	Frequency
On my phone	335 (81.5%)
Tablet	109 (26.5%)
Laptop	361 (87.8%)
Desktop	123 (29.9%)
Other (please specify)	11 (2.7%)
N = 411	

Notes: a. Dichotomy group tabulated at 1.

Table 5.13

Frequency distribution of number of times of Online Purchases by respondents

Times of online purchase ^a	Frequency
1-5 times	273 (74.8%)
6-10 times	57 (15.6%)
11-15 times	25 (6.8%)
More than 15 times	16 (4.4%)
N = 365	

Notes: a. Dichotomy group tabulated at 1.

Table 5.13 displays frequencies of students online purchase activity. The table reveals that a great majority of students (74.8 percent) purchased something between 1-5 times in a month in the past year. This is followed by 15.6 percent (57 students) who purchased something between 6-10 times per month in the past year. The least number of times students purchased something online is more than 15 times which has a frequency of just about 4 percent (16 students). The table thus reveals that even though almost all students undertake online purchases, most of them do that between 1-5 times in a month.

Table 5.14

Frequency distribution of Online Safety precautions adopted by respondents

<u>Online safety Precaution^a</u>	<u>Frequency</u>
I do not respond to anonymous emails	334 (82.5%)
I always shop on safe sites	314 (77.5%)
I don't use public computers for banking transactions	313 (77.3%)
I check my credit/bank statement frequently	291 (71.9%)
I don't run unknown applications on my computer	257 (63.5%)
I always ensure I have an updated anti-virus	167 (41.2%)
I change my passwords frequently	51 (12.6%)
Other (please specify) ...	15 (3.7%)
I don't employ any safeguard online	13 (3.2%)
N = 405	

Notes: a. Dichotomy group tabulated at 1.

Table 5.14 on the other hand shows the various online safety precautions utilised by respondents. The predominant option is not responding to anonymous emails with a frequency of 82.5 percent (334 students). Another popular precautionary measure is always shopping on safe sites and not using public computers for banking, with frequencies of 77.5

and 77.3 percent respectively. However, 13 students (3.2 percent) do not employ any precautionary measure when online.

5.4. Hypotheses testing

5.4.1. Hypotheses 1, 2 and 4

Table 5.15 presents results of combined binary logistic regression analysis of data in respect of hypotheses 1, 2 and 3. This is because the hypotheses in question have the same outcome variable (that is, fear of credit/debit card fraud victimisation). Given that the dependent variable in all three cases is a binary variable, binary logistic regression has been utilised to test these hypothesis.

5.4.1.1. Results for hypotheses 1, 2 and 4: Logistic Regression

Table 5.15

During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?

Predictor Variables	B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
							Lower Bound	Upper Bound
Intercept	-1.856	2.960	.393	1	.531			
[Q1=1]	.340	.387	.501	1	.384	1.405	.616	2.808
[Q1=2]	-.523	.739	.610	1	.476	.593	.132	2.390
[Q1=3]	0 ^b	.	.	0
[Q9=1]	1.177	.431	7.475	1	.006**	3.246	1.396	7.550
[Q9=2]	0 ^b	.	.	0
[Q22_New=1]	-.009	.290	.001	1	.976	.991	.561	1.751
[Q22_New=2]	0 ^b	.	.	0
[Q23=1]	-.284	.607	.218	1	.640	.753	.229	2.476
[Q23=3]	-.005	.536	.000	1	.993	.995	.348	2.847
[Q23=4]	0 ^b	.	.	0
[Q24=1]	-.887	1.521	.340	1	.560	.412	.021	8.120
[Q24=5]	-.762	1.578	.233	1	.629	.467	.021	10.284
[Q24=9]	0 ^b	.	.	0
[Q25_New=1]	-.268	.707	.143	1	.705	.765	.191	3.058
[Q25_New=2]	0 ^b	.	.	0
[Q26=1]	-.636	.532	1.430	1	.232	.529	.186	1.502
[Q26=2]	0 ^b	.	.	0
[Q27_New=1]	-.443	.746	.353	1	.553	1.558	.361	6.727
[Q27_New=2]	-.658	.523	1.582	1	.208	.518	.186	1.4449
[Q27_New=3]	-.065	.452	.020	1	.886	.938	.873	2.272
[Q27_New=4]	.291	.524	.308	1	.579	1.337	.479	3.738
[Q27_New=5]	0 ^b	.	.	0
[Q28_New=1]	-.289	1.589	.033	1	.856	.749	.033	16.873
[Q28_New=2]	0 ^b	.	.	0
[Q29=1]	.195	.417	.220	1	.639	1.216	.537	2.751
[Q29=3]	.533	.448	14.18	1	.234	1.704	.709	4.098
[Q29=5]	0 ^b	.	.	0
[Q30=1]	.119	.362	.108	1	.742	1.127	.554	2.289
[Q30=2]	0 ^b	.	.	0
[Q31=1]	.451	.290	2.421	1	.120	1.569	.890	2.768
[Q31=2]	.345	.542	.404	1	.525	1.411	.488	4.084
[Q31=3]	0 ^b	.	.	0

a. The reference category is: No.

b. This parameter is set to zero because it is redundant

* $p < .05$

As revealed in Table 5.15, the variable knowledge of cybercrime (Q1) is non-significant, irrespective of the level of the variable. The reference category here is belief that cybercrime is both cyber-enabled and cyber-dependent (coded 3). When level one of the

independent variable (that is, cyber-enabled) is compared with the reference category, a p-value of .384 is observed, which then translates into .340 as estimate of the coefficient on the logit scale. This also corresponds to an odds ratio of 1.405. The non-significant p-value means that controlling for all other variables, there is no significant relationship between knowledge of cybercrime and fear of credit/debit card fraud victimisation. The odds ratio of 1.405 specifically implies that, the reference category have the lower proportion, hence less fear relative to students who hold the view that cybercrime is only cyber-enabled. It also implies the chances that a student will have fear increases when a student believes cybercrime is only cyber-enabled. Also when the second level or category (that is, cyber-dependent) of the independent variable is compared with the reference category, a p-value of .476 which corresponds to -.523 as an estimate of the coefficient on the logit scale and an odds ratio of .593 are observed. The p-value as observed indicates that controlling for all other variables, there is no significant relationship between knowledge of cybercrime and fear of credit/debit card fraud. The odds ratio also means that, the reference category have the larger proportion, hence more fear compared to students whose knowledge of cybercrime is that of only cyber-dependent. It also implies the probability that a student will have fear falls when the student believes cybercrime is only cyber-dependent.

Table 5.15 also reveal that only predictor variable experience of victimisation (Q9) is significant with a significant p-value of .006. Specifically, the p-value of experience of victimisation corresponds to 1.177 as an estimate of the coefficient on the logit scale which then translates into odds ratio of 3.246. Given the significant p-value, it implies that controlling for other variables in the model, there is a significant relationship between prior experience of victimisation and fear of future credit/debit card fraud victimisation. And given that the reference category for this variable is No (coded 2), the finding specifically means that students with prior experience of victimisation (Yes) have a larger proportion and hence

are more fearful of credit/debit card fraud victimisation compared to students without prior experience. The odds ratio of 3.246 means that the probability of the event occurring with a unit increase in the independent variable is higher than at the original value of the independent variable. In other words, the chances of a student becoming fearful of credit/debit card fraud victimisation increases with experience of victimisation.

The remaining variables in the question do not add significantly to the prediction. The table however, also demonstrates that the other variables even though not significant, do have some relationship with the dependent variable, one way or the other. On the bases of the information from the table, we can therefore make predictions in respect of hypotheses one, two and four.

5.4.1.2. Predictions from Hypotheses testing: Hypotheses 1, 2 and 4

Hypothesis 1: Table 5.15 reveal that the values of the test statistic or the p-values for the tests are .384 and .476, which are both greater than the significance level (0.05). Therefore, the sample does not provide enough evidence to reject the null hypothesis. Hence we fail to reject the null hypothesis and conclude that, students' knowledge/perception of cybercrime does not significantly affect their fear of credit/debit card fraud victimisation at 95% level of confidence.

Hypothesis 2: From the multiple predictor variables as revealed in Table 5.15, none of the socio-demographic variables is significant, that is, they all have p-values $>.05$. The variables here include gender, age, marital status, ethnic identification, family income among other socio-demographic variables. Therefore the sample does not provide enough evidence to reject the null hypothesis. Hence we fail to reject the null hypothesis and conclude that, socio-demographic factors do not make a significant difference to students' fear of credit/debit card fraud (females, older students, single, non-whites with higher income have

no more significant fear compared to males, younger, non-single, white students with less income) at the 95% level of confidence

Hypothesis 4: Table 5.15 also reveal that the value of the test statistic or the p-value for the test is .006, which is less than the significance level ($p < .05$). Therefore the sample does not provide enough evidence to accept the null hypothesis. Hence we fail to accept the null hypothesis and conclude that, there is a significant difference in fear of credit/debit card fraud between students with prior experience of victimisation compared to students without experience of victimisation at 95% level of confidence.

5.4.2. Hypotheses testing: Hypothesis 3

5.4.2.1 Results for hypothesis 3: Logistic Regression

Table 5.16

Compared to other crimes (physical crimes), do you feel more at risk of Credit/Debit Card fraud?

Predictor Variables	B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
							Lower Bound	Upper Bound
Intercept	-18.691	1.334	196.260	1	.000			
[Q13_New=1]	.441	.276	2.554	1	.110	1.555	.905	2.672
[Q13_New=2]	.110	1.002	.012	1	.912	1.117	.157	7.964
[Q13_New=3]	-.062	.550	.013	1	.910	.940	.320	2.761
[Q13_New=4]	0 ^b	.	.	0
[Q15=1]	19.261	1.476	170.270	1	.000*	2.318E8	12840188.900	4.183E9
[Q15=2]	18.727	1.349	192.654	1	.000*	1.359E8	9652969.858	1.912E9
[Q15=3]	18.099	.000	.	1	.*	72502928.730	72502928.730	72502928.730
[Q15=4]	0 ^b	.	.	0
[Q16=1]	-.730	.305	5.733	1	.017*	.482	.265	.876
[Q16=2]	-.114	.293	.152	1	.697	.892	.502	1.584
[Q16=3]	-.419	.275	2.327	1	.127	.657	.383	1.127
[Q16=4]	0 ^b	.	.	0
[Q17=1]	.703	.355	3.923	1	.048*	2.020	1.007	4.051
[Q17=2]	0 ^b	.	.	0

a. The reference category is: No.

b. This parameter is set to zero because it is redundant.

* $p < .05$

From Table 5.16, predictor variables frequency of internet use (Q15), time spent on the internet at any given time (Q16) and online purchase (Q17) are all significant, with significant p-values of .000, .017 and .048 respectively. More specifically, with frequency of internet use (Q15), all the major categories are significant with the same p-value (.000). The implication is that controlling for all other variables, there is a significant relationship between students' frequency of internet use and their risk of credit/debit card fraud. The reference category for this variable is Monthly internet access (coded 4). When you compare

the first main category of the variable (Once Daily) with the reference category, the odds ratio is 2.318. This implies that the reference category has the lower proportion and hence, have less risk of credit/debit card fraud compared to students who access the internet daily (everyday). The odds ratio further means that, the probability of a student standing the risk of credit/credit card fraud increases with daily internet use. When the second main category of the variable (Several times in a day) is compared with the reference category, the odds ratio is observed to be 1.359. Here the converse is also true, that is, the main category has the higher proportion and hence, stands more risk of credit/debit card fraud compared to students who access the internet monthly. The odds ratio also implies that the probability of a student standing the risk of credit/debit card fraud increases when a student accesses the internet several times in a day. Then again with the third main category of the variable (Weekly internet access), the odds ratio is even bigger attaining a value of 72502928. This means that the main category have an extremely larger proportion hence, stand more risk of credit/debit card fraud compared to students who access the internet monthly. This further implies that the probability of a student standing the risk of credit/debit card fraud increases when a student access the internet weekly.

Table 5.16 also reveals that time spent on the internet (Q16) is significantly related to risk of credit/debit card fraud. When the first main category of the variable (Less than 30 minutes) is compared with the reference category (Over 2 hours), a p-value of .017 which translates into -.730 as an estimate of the coefficient on the logit scale, and an odds ratio of .482 are observed. The p-value implies that controlling for all other variables, there is a significant relationship between time spent on the internet and students risk of credit/debit card fraud. The odds ratio on the other hand means that the reference category has the higher proportion hence, stand more risk compared to students who spend less than 30 minutes on the internet. The odds ratio also imply that the probability of a student to experience the risk

of credit/debit card fraud falls when the student spends less than 30 minutes on the internet. On the other hand when the second main category of the variable (Over 30 minutes but less than an hour) is compared with the reference category, a p-value of .697 corresponding to -.114 as an estimate of the coefficient on the logit scale, and an odds ratio of .892 are observed. The observed p-value indicates that controlling for all other variables, there is no significant relationship between time spent on the internet and students risk of credit/debit card fraud. The odds ratio on the other hand means that the reference category has the larger proportion hence, stand more risk compared to students who spend more than 30 minutes but less than an hour on the internet. This further implies that the probability of a student standing the risk of credit/debit card fraud falls when the student spends more than 30 minutes but less than an hour on the internet.

Finally when the third main category of the variable (Between 1 and 2 hours) is compared with the reference category, we observe a p-value of .127 which then translates into -.419 as estimate of the coefficient on the logit scale, and an odds ratio of .657. The p-value here also means that, controlling for all other variables, there is no significant relationship between time spent on the internet and students risk of credit/debit card fraud. The odds ratio on the other hand means that the reference category still has the larger proportion hence stand more at risk compared to students who spend between 1 and 2 hours on the internet. The odds ratio further implies that the probability of a student standing the risk of credit/debit card fraud also falls when the student spends between 1 and 2 hours on the internet.

Furthermore, Table 5.16 again reveals that online purchase (Q17) is also significant. The reference category here is No and is compared with the main category (Yes). For this variable, a significant p-value of .048 which translates into .703 as an estimate of the coefficient on the logit scale, and an odds ratio of 2.020 are observed. The significant p-value

means that controlling for all other variables, there is a significant relationship between online purchase and student's risk of credit/debit card fraud. The odds ratio specifically indicates that the main category has the larger proportion hence, stand more at risk compared to students who have not used the internet for online purchase. The odds ratio also implies that the probability of a student standing at risk of credit/debit card fraud increases when the student uses the internet for online purchases.

On the other hand Table 5.16 reveals that the other predictor variable in the table - place of regular internet access (Q13), is non-significant and does not add significantly to the prediction. The reference category for this variable is 'Home' (coded 4). Given that none of the categories of the variable has a $p\text{-value} < .05$, it implies that controlling for other variables, there is no significant relationship between place of internet access and risk of credit/debit card fraud.

On the other hand Tables 5.17, 5.18 and 5.19 present's results for the other predictor variables (medium of internet access - Q14, frequency of online purchase - Q18 and online safety precautions - Q19) which are multiple response questions, for hypothesis three.

Table 5.17

Cross tabulation of the relationship between medium of internet access and risk of Credit/Debit card fraud victimisation

How do you access the internet	Compared to other crimes (physical crimes), do you feel more at risk of Credit/debit card fraud?	
	Yes	No
On my phone	207 (61.8%)	128 (38.2%)
Tablet	67 (61.5%)	42 (38.5%)
Laptop	222 (61.5%)	139 (38.5%)
Desktop	83 (67.5%)	40 (32.5%)
Other (please specify)	6 (54.5%)	5 (45.5%)
N = 411		

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

Multiple response Table 5.17 presents a cross tabulation of the relationship between medium of internet access and risk of credit/debit card fraud victimisation. As revealed in Table 5.17, majority (61.8 percent) of students who access internet on their phone feel at risk compared to 38 percent (128 students) not feeling at risk of credit/debit card fraud. For students accessing internet through their tablets, (61.5 percent) feel at risk whereas 42 students (38.5 percent) do not feel at risk of credit/debit card fraud. Again for students who access internet on a laptop, another majority (222 or 61.5 percent) of students feel at risk whilst about 39 per cent (139 out of 361) of students do not feel at risk of credit/debit card fraud. Furthermore, a vast majority (about 68 percent) of students who access internet on a desktop feel at risk compared to only 32 percent who do not feel at risk. Finally, for students who access internet through other interfaces, more than half (54.5 percent), report feeling at risk whereas about 45.5 percent of students report not feeling at risk. On the whole, the table

therefore reveals that students generally feel at risk of credit/debit card fraud victimisation irrespective of the medium of internet access. In other words, medium of internet access is overwhelmingly related to risk of credit/debit card fraud victimisation.

Multiple response Table 5.18 on the other hand presents a cross tabulation of the relationship between online purchase and risk of credit/debit card fraud victimisation. The table reveals that out of (273) students who purchased items online between 1-5 times, about two thirds (63.7 percent or 174) felt at risk while 36.3 percent (99) do not feel at risk. Also, more than half (32 students or 56.1 percent) of students who purchased items online between 6-10 times, feel at risk while 25 students (about 44 percent) do not feel at risk. Then again out of a total of 25 students who purchased items online between 11-15 times, a vast majority (72 percent) feel at risk compared to 28 percent who do not feel at risk of credit/debit card fraud. Furthermore, for students who carried out more than 15 instances of online purchase a month in the past year, about 63 percent (10 students) feel at risk whilst 37 percent of them do not feel at risk of credit/debit card fraud. Once again the conclusion from the table is that in all instances of online purchase, majority of students feel at risk of credit/debit card fraud. In other words, frequency of online purchase is overwhelmingly related to risk of credit/debit card fraud among students.

Table 5.18

Cross tabulation of the relationship between number of times of online purchase and risk of Credit/Debit card fraud victimisation

Number of online purchase	Compared to other crimes (physical crimes), do you feel more at risk of Credit/debit card fraud?	
	Yes	No
1-5 times	174 (63.7%)	99 (36.3%)
6-10 times	32 (56.1%)	25 (43.95%)
11-15 times	18 (72.0%)	7 (28.0%)
More than 15 times	10 (62.5%)	6 (37.5%)
N = 365		

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

Multiple response Table 5.19 presents a cross tabulation of the relationship between online safety precautions and risk of credit/debit card fraud victimisation. Of a total of 314 students who shopped on safe sites, 197 students representing about 63 percent feel at risk compared to 117 students (37 percent) not feel at risk of credit/debit card fraud victimisation. Also for students who always ensure they have an updated anti-virus, more than half, that is about 65 percent (108 out of 167) feel at risk while 35 percent (59 students) feel no risk. Again out of a total of 313 students who avoid using public computers for online shopping and banking transactions, about 63 percent (196 students) feel at risk while 37 percent (117 students) do not feel at risk. Furthermore, of a total of 334 students who do not respond to anonymous emails, majority (63 percent or 209 students) feel at risk compared to 37 percent (124 students) who do not feel at risk of credit/debit card fraud. Moreover, for students who do not run unknown applications on their computers, 60 percent feel at risk while about 40 percent (102 students) do not feel at risk of credit/debit card fraud. Again of the 51 students who changed their passwords frequently, about two thirds (67 percent) feel at risk while 33

percent do not feel at risk. Additionally for students who frequently check their credit report or bank statement, about 63 percent (183 students) feel at risk compared to 37 percent (108 students) not feeling at risk. On the other hand of the 15 students who used other precautions or mechanisms, 33 percent feel at risk compared to about two-thirds (67 percent) not feeling at risk of credit/debit fraud. Finally for students who do not use any safety precaution, about 54 percent (7 students) report feeling at risk compared 46 percent (6 students) not feeling at risk.

Table 5.19

Cross tabulation of the relationship between Online safety precautions and risk of Credit/Debit card fraud victimisation

Online safety precautions	Compared to other crimes (physical crimes), do you feel more at risk of Credit/debit card fraud?	
	Yes	No
I always shop on safe sites	197 (62.7%)	117 (37.3%)
I always ensure I have updated anti-virus	108 (64.7%)	59 (35.3%)
I don't use public computer for banking	196 (62.6%)	117 (37.4%)
I don't respond to anonymous emails	209 (62.6%)	125 (37.4%)
I don't run unknown applications	155 (60.3%)	102 (39.7%)
I change my passwords frequently	34 (66.7%)	17 (33.3%)
I check my credit/bank statement frequently	183 (62.9%)	108 (37.1%)
Other (please specify)	5 (33.3%)	10 (66.7%)
I don't employ any online precaution	7 (53.8%)	6 (46.2%)
N = 405		

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

Table 5.19 reveals that all the various online safety precautionary measures, except the other category, are positively and progressively related to risk of credit/debit card fraud. This means that the more a student adopts online safety precautions, the more risky they feel for credit/debit card fraud. However, the table also reveal that students who do not use any online safety precaution, also report experiencing a high level of risk. More than half of students in this category (53.8 percent) specifically feel at risk of credit/debit card fraud victimisation, with the remaining 46.2 percent not feeling at risk.

5.4.2.2 Predictions from Hypotheses Testing: Hypotheses 3

Based on the binary logistic regression Table 5.16 and multiple choice Tables 5.17, 5.18 and 5.19, we can make predictions in respect of hypothesis number 3.

Hypothesis 3: From the binary logistic regression Table 5.16, all predictor variables (except place of internet access, significance values $p > 0.05$, produced test statistic with values below the 0.05 significance level (that is, 0.00 for frequency of internet use; 0.01 for time spent on the internet and 0.04 for online purchase). Similarly multiple choice tables 5.17, 5.18 and 5.19 all represent positive relationships. Therefore we can generally conclude that the sample does not provide enough evidence to accept the overall null hypothesis. Hence we fail to accept the null hypothesis and conclude that, internet use behaviours significantly affect students' risk of credit/debit card fraud victimisation at the 95% level of significance.

5.5. Chapter Summary

The chapter has presented findings from various statistical tests in relation to key variables. Both descriptive information and results from hypotheses testing have been provided. Descriptive information included both univariate and bivariate findings. Information on students' internet access revealed students accessed internet through all the various media, but with majority of students accessing internet on their laptops. Online

purchasing activity was also a common practice among most students, and with students adopting various types of online safety precautions while online.

Results of bivariate tests also reveal gender was related (in a non-significant way though) to fear of credit/debit card fraud, with female students expressing relatively more fear. However, none of studentship status (part time or full time), residency status (domestic or international) and place of residence (campus or off campus residence) were found to be related to students fear of credit/debit card fraud. Likewise, employment/work status, income, age and level of studies were all found to be unrelated to students' fear of credit/debit card fraud. Finally, marital status and ethnic identification were also both found to be unrelated to students' fear of credit/debit card fraud victimisation.

Finally, results of hypotheses testing, using both binary logistic regression and chi-square reveal support for hypotheses 3 and 4. On the other hand, both hypotheses 1 and 2 did not find support from the results of the test. In other words, internet use behaviours and experience of victimisation are both significant and positively associated with students' fear and their risk of becoming victims of credit/debit card fraud. However, knowledge of cybercrime and socio-demographic background are both non-significant and make no significant difference to students fear and risk of credit/debit card fraud victimisation. The next chapter focuses on critical analysis of the results presented in this chapter, in light of the research questions and the existing literature.

CHAPTER 6

ANALYSIS AND DISCUSSION

6.0. Introduction

This chapter presents analysis of the key findings in relation to the variables of interest and hypotheses. The discussion is guided by the theoretical framework of Beck's risk society and links the various hypotheses to the research. Eventually, the overall analysis is linked back to the key research question.

6.1. Impact of students' knowledge/perception of cybercrime on fear of Credit/Debit card fraud

Table 5.15 revealed interesting findings in respect of students' knowledge of cybercrime and its relation to fear of cybercrime. The hypothesis that fear of cybercrime will be significantly impacted by students' knowledge was not supported. It is noteworthy that though non-significant, majority of students (83.4%) demonstrate what may be termed a comprehensive knowledge of cybercrime (see Table 5.11). The term comprehensive knowledge refers to the understanding of cybercrime as both cyber-enabled and cyber-dependent, and covers the broader spectrum of the components of cybercrime as identified earlier in the literature (McGuire & Dowling, 2013). A perspective of cybercrime which points to either view is, consequently narrow. This supports the outcome of the logistic regression analysis, where the reference category (the view that cybercrime is both cyber-enabled and cyber-dependent) is observed to have a lower proportion in one step and a larger proportion at the next step. A lower proportion means less fear while a larger proportion means more fear.

The finding on knowledge and fear, however, contradict the literature on the theme. In their Slovenian study, Mesko and Bernik (2011) found that knowledge of cybercrime was significant in reducing people's fear of cybercrime. Their view was premised on the fact that

awareness and fear of cybercrime are linked to people's knowledge of cyber threats.

However, their sample was a heterogeneous sample comprising of diverse sections of the population. The current finding is relevant and can be generalised to student populations given the homogeneity of the sample (university students).

The implication from the above is that, other factors account for fear but not knowledge. Alternatively the non-significance of knowledge can be explained away by an examination of the nature of the crime involved. Essentially the basic nature of credit/debit card fraud is that it is a crime committed not in the physical visible space, but in cyberspace. The frequency of comprehensive cybercrime knowledge (83.4%) suggests students have a basic understanding of this fact. The lack of visibility, therefore, indicates students are not able to immediately appreciate the dangers of this crime. Consequently knowledge alone, even though important, may not significantly affect fear. For one to really appreciate the dangers of this crime will pre-suppose a first-hand experience, and not just having what may be termed 'theoretical' knowledge. A potential significant explanatory factor could be victimisation experience, which itself is one of the indicator variables explored further down in this chapter. Another potential factor affecting significance of the knowledge variable, could be the likely mitigating role of perceptions of media hype. There is the view out there that actual crime prevalence is less relative to what is mostly reported. Media hype linked to sensational media reporting of criminal victimisations is thus believed to portray an exaggerated picture of the real crime situation. Therefore students holding onto this view of media hype may actually end up not having much fear of credit/debit card fraud victimisation, despite their comprehensive knowledge. This explanation will especially hold true when students possess only 'theoretical' knowledge. Even as risk is system immanent (inherent to internet use), as Beck explains, by not demonstrating fear after possessing comprehensive knowledge, indicates an aspect of agent reflexivity. Reflexivity because the

act of choosing not to have fear, after possessing knowledge of cybercrime, would entail a mental evaluation of the extent of risk and probability of victimisation before arriving at the conclusion that a given risk rate does not warrant fear. This aspect of reflexivity would even become more pronounced and receive centre stage, after students have taken into consideration and discounted the media hype.

6.2. Impact of Socio-demographic factors on Students' fear of Credit/Debit card fraud

As revealed in Table 5.15 under the findings and interpretation section, none of the socio-demographic factors (variables) of students turned out to be a significant predictor of fear of credit/debit card fraud victimisation. More specifically, gender, age, marital status, ethnic identification and family income among other independent variables (socio-demographic factors) into the model are all non-significant predictors contrary to the hypothesised prediction.

These findings both support and contradict the existing literature in equal measure. Fundamentally, the findings contradict the literature that gender matters and with females having more fear than their male counterparts (Callanan et al., 2015; Alshalan, 2006; Anderson, 2006; Fox, 2001). It further contradicts the literature that older and more educated respondents have less fear compared to other age groups (Mesko et al, 2011). The finding also goes contrary to Anderson's findings on predictors of cyber-identity theft victimisation in the USA (Anderson, 2006). Anderson found that age, gender and income were significant predictors of cyber-identity theft victimisation, with younger adults, women and affluent people more likely to be victims. Similarly the current finding is at variance with study of identity theft victimisation in Australia (Australian Bureau of Statistics, 2008). It was established that gender, age, education and income were significant predictors of identity theft victimisation, with males, aged between 25-44 years, with higher educational

qualifications and with the highest weekly incomes being more likely to be victims (Australian Bureau of Statistics, 2008).

The finding that gender is a non-insignificant predictor of fear, however, corroborates some of the literature on fear of cybercrimes. For example gender was found to be a poor predictor of fear of cyber identity theft victimisation, accounting for less than half of the variation in the fear of cyber identity theft victimisation (Roberts et al., 2013). This finding is significant and finds justification in Beck's theory. The fact risks come as unintended consequences from the continual processes of techno-scientific developments, means the threat of credit/debit card fraud victimisation is experienced as gender-blind. Consequently fear for such crime is generally unmitigated by gender distinctions.

Females' disproportionately high fear has been attributed to the "shadow of sexual assault hypothesis" (Ferraro, 1995; 1996). The argument put forward here is that women's fear of rape masks their fear of other forms of victimisation, with the spectre of being raped remaining an "ever-present" concern among women (Ferraro, 1995; 1996). Others have also attributed the heightened female fear to the fact females are incapable of defending themselves in physical attack (Callanan et al., 2015; Hale, 1996). As previously pointed out, however, both of these explanations are likely only plausible for fear of physical or 'conventional' crimes, especially sexual assault related fears for the incapability for personal defence explanation. This is because these (physical or 'conventional') crimes are amenable to geographic boundary limitations and relies on the physical or personal contact between offender and victim. However, this position is untenable for non-sexual assault related fears and in this context credit/debit card fraud. This type of crime as revealed under the key distinguishing characteristics of cybercrimes is not susceptible to geographic boundary limitations and can occur multiple times at the same time across different locations. Perhaps its remote application within the realm of cybercrime can only be limited to sexual assault

related cybercrimes. In this way findings that females exhibit more fear of cybercrime and specifically demonstrate more concern for online credit card theft (Alshalan, 2006; Fox, 2001), are untenable.

Feminists' criminologists, on the other hand, have also challenged the gendered difference, and especially females increased fear of crime. Their response is that gender is socially constructed, with "gender differences in child and adult socialization" accounting for the gendered difference in fear of crime (Callanan et al., 2015:322). Implicit in the feminists argument here is an implied significant role for patriarchy. Conversely, the non-significance of gender in this study is, more consistent both with the nature of credit/debit card fraud and the theory of risk society. This finding can be accounted for by the fact cybercrimes by their defining attributes occur in the cyber world where, the physical proximity of offender and victim is not applicable. As a result, such crimes can take place simultaneously at multiple locations and at a very fast pace (velocity). The absence of the physical proximity therefore, means that, it is immaterial to a cyber fraudster whether a potential victim identifies as male or female.

In light of the literature, the current finding is important and adds relevant dimensions to the literature on fear of crime, and more specifically fear of cybercrime. It is important because it validates previously disputed works such as that by Roberts et al. (2013). Significantly it also adds a unique perspective from the point of view of the explanations offered in the current study. In the broader perspective, however, the current finding points to the fact that the relationship between socio-demographic variables and fear of criminal victimisation remain fuzzy, calling for a more nuanced analysis of key socio-demographic variables such as age, gender, income, ethnicity among others, and fear. In the context of gender for example, specific attention can be placed on women (females) and their social context.

Having said these, it is possible some of the observed differences with regards to the significance of socio-demographic variables on fear of crime, and for this study, credit/debit card fraud victimisation, could partly be attributable to differences in choice of sample as well as the characteristics of the chosen samples. Most of the studies cited in the literature were carried out in broader contexts with heterogeneous samples. The fact the current study was conducted on a university campus and restricted to only students (homogeneous sample) therefore means our sample will differ in unique ways from heterogeneous samples. Also given that most of the socio-demographic variables are significant in the context of physical place-based or ‘conventional’ crimes, the findings imply that the context of crime is important and determines which factors are significant or not.

6.3. Impact of Internet use behaviours on students’ risk of credit/debit card fraud victimisation

The data has revealed that internet use behaviours significantly predict students’ risk of credit/debit card fraud victimisation. The various internet use variables overwhelmingly support the prediction as revealed in the findings and interpretation section. This finding is in line with the hypothesised prediction and as well in consonance with predictions of the theoretical framework.

As students interact with the internet on an increased frequency, they become exposed to possibilities of victimisation and hence their increased risk. The risk of victimisation exists in this wise, because cyber fraudsters tend to have more possibilities of tracking the trajectories of a frequent internet user. So even when an internet user is convinced of the safety and security of the online platform, some appreciable amount of risk is still prevalent. This is because risk is ‘system’ immanent (Beck, 1992), that is, it is inherent to the online platform. Also the same or similar logic applies to time spent on the internet as with

frequency of internet use. Going online frequently and spending more time at each given online visit, both carry the same profile in terms of exposing patrons to risk of victimisation.

Significantly online purchase activity also raises individuals risk profile in terms of credit/debit card fraud victimisation. Through online purchase, an individual dispenses with certain critical information in terms of address and bank card details. Even though risky, however, this information is necessary to successfully complete any online purchase transaction. Meanwhile doing so also invariably means the person's identity is released onto the cyberspace – the 'invisible' world characterised by incessant activity. Consequently it becomes predictable when a person report feeling at risk after undertaking online transactions. This finding is supported by the literature on fear of cybercrime. It had been established that the more people divulge their credit/debit card information, the more they are at risk of becoming victims of cybercrime (Alshalan, 2006; Anderson, 2006).

Again as observed under frequency of internet use and time spent on the internet, frequency of online purchase also works in a similar fashion as online purchase activity. The more an individual undertakes online purchasing activity, the more the person becomes exposed to the risk of victimisation. Significantly, however, as the data revealed, any number of times of online purchase exposes students to risk of credit/debit card fraud victimisation. The underlying factor here is mainly the activity of online purchase, and not so much about the frequency, even though an increased frequency will tend to mean an increased risk. The bottom line is that online transactions involve dispensing with certain vital information, which exposes the person involved.

The findings on internet use behaviours, as seen from the foregoing have all been supported by the literature. Alshalan found that "people who use the Internet more frequently, stay online longer, and engage in Internet activities that involve divulging their id information

or financial information are more likely to be victims of Cyber-Crime” and in this case credit/debit card fraud (2006:133).

As well as the above, the various media of internet access have all been shown to be overwhelmingly related to increased risk of credit/debit card fraud victimisation. Whether the media is phone, tablet, laptop, desktop or other media, an overwhelmingly positive relation with increased risk is observed, with more than 50 percent affirmative responses in all the cases. The implication of such finding is that, the medium of internet access is inconsequential and rather increases students’ risk of victimisation. Indeed, if anything at all, the overwhelming nature of the statistics in the various cases only point to a very strong positive relationship between medium of internet access and risk of victimisation. However, one would have thought a priori that media such as phone or personal laptops and tablet would have been associated with less or reduced risk. This thinking is motivated by the view that these media are basically under the control of the owner, and so he/she will have exclusive access and control over its use. But as credit/debit card fraud is a criminal activity in cyberspace, it turns out that even personal ownership of internet access gadgets do not absolve an individual of the risk of victimisation. This therefore tends to point to the theoretical prediction, that is, the medium of internet access will not necessarily reduce people’s risk. The underlying point is that risk is ‘system’ immanent and universalising (increasingly global) and thus it is inescapable (Beck, 1992).

Furthermore, online safety mechanisms also appear to overwhelmingly predict increased risk of credit/debit card fraud victimisation, with all the various online safety mechanisms associated with increased risk (more than 50 percent in all cases). This means that even though students employ safety precautions as a demonstration of their reflexivity, it still does not take away their feelings of risk. This observation elicits the argument as to whether behaviour modification is a response to fear, or it is simply a precaution. This

finding however, points to the fact that in either of both instances, the basic element of feelings of risk is not done away with, rather it continually prevails. The caveat to the safety mechanisms, however, is the ‘other’ mechanisms option. Most notably, students adopting this set of mechanisms tend to experience reduced risk (66.7 percent not experiencing risk). Importantly, pay pal is the predominant option under this category, as revealed in the data. The implication from this category is that students tend to have a very high level of trust in the protection offered by pay pal, for which reason they report experiencing less risk when using pay pal for online payments. In essence, pay pal defies the predominant hypothesised prediction. Consequently, it is safe to conclude that this is simply a case of an exception to the rule rather than the norm.

However, the finding in relation to adoption of safety mechanisms contradicts some of the prevailing literature. Instead of the overwhelming positive relationship observed between online safety precautions and increased risk of victimisation, Anderson (2006:161) argued that consumer precautions, such as regularly monitoring account activity and checking credit report, minimises the risk of victimisation if it cannot completely be avoided. However, risk minimisation through consumer adoption of precautionary measures, reflects consumer reflexivity and thus an act in governing structural constraints. This basically underscores an important element of the risk society theory – agent reflexivity, where actors tend not to be bounded by structural constraints (Beck, 1992). The view is that the pervasiveness of risks, resulting from unintended consequences of technological development, does not mean actors are automatically given to the risks. Instead, as the risk theory holds, actors attempt to exert control over the pervasive risk (structural constraints) by adopting some measures to limit the potency of these risks. And by so doing, it demonstrates agent reflexivity as predicted by Beck (1992).

The adoption of online safety precautions and its relationship to risk also manifests the theoretical predictions of the world risk society. Risk theory postulates that actors or human agents are reflexive, that is, they are not bounded by structural constraints (Beck, 1992). So in response to the inherently risky nature of cyberspace, in terms of the possibilities of credit/debit card fraud victimisation, people adopt these precautionary measures as a realisation of their own reflexivity. However, as observed from the data, these measures do not do away with the inherent risk, and hence the feelings of risk. It thus however, prevents or reduces eventual victimisation.

From the foregoing, the hypothesised prediction that internet use behaviours increase student's risk of credit/debit card fraud victimisation has been generally proven to be true. In doing so, the theoretical position that risk is inescapable in the world risk society is confirmed. It further demonstrates that, while risk remains generally inescapable, the defining element as to whether an agent moves from the threshold of risk to real victimisation is about reflexivity. Reflexivity in this context, however, does not suggest the absence of risk.

6.4 Impact of past experience of victimisation on fear of credit/debit card fraud victimisation

The results from the findings section revealed that experience of victimisation significantly predict fear, and specifically, students with victimisation experience report heightened fear compared to students without victimisation experience. The finding confirms the hypothesised prediction and finds support in the literature (Alshalan, 2006; Yu, 2014). However, some prevailing literature contradicts the current findings (Whitrod & Maxfield in Carcach et al., 1995).

Having had prior experience of victimisation elicits insecurity and consequently fear in a person, especially as the person gets into contact with the internet following the initial victimisation. The source of insecurity and hence fear, results from the constant state of flux

which characterises cyberspace. The lack of physicality to this space also makes it a challenge for people, even after they employ safeguards. A further possible explanation for the fear could be due to the fact that sometimes people only realise they have been victimised several weeks after the fact. They only become aware after receiving or checking their bank statements. Realising one's victimisation this way will tend to leave such a person in a constant state of fear.

However, the literature on the predictive significance of victimisation experience remains contentious. Even though others have also established victimisation experience as significantly predicting fear of cybercrime (Alshalan, 2006), some literature argue that the predictive influence of victimisation experience is not straightforward. Instead, it is argued that it depends on the type of cybercrime (Yu, 2014). This position however, appear to be in line with the direction of the current study. This research is underpinned by the view that lumping predictors of fear of crime into overarching or general categories, is not helpful. Instead, the present study takes the view that predictors should be sought for specific types of crimes. To this extent, the fact victimisation experience has been found to significantly predict fear of credit/debit card fraud is significant. This is because credit/debit card fraud is just but one of the several types of cybercrimes.

The current finding, however, challenges the position that fear is unrelated to patterns of victimisation or actual victimisation, and that it is instead the result of "perceived vulnerability based on subjective judgements of personal risk" (Whitrod & Maxfield in Carcach et al., 1995:273). This position brings into focus, argument about the perception of disorders which gives rise to feelings of vulnerability, and hence, fear. The argument is that the neighbourhood context influences fear in important ways. Consequently, disruptive and disorderly neighbourhoods generate feelings of vulnerability – real or hypothetical - among residents. This view especially hold true for physical environments but also true for the cyber

environment due to the prevalence of computer viruses of different kind. This argument is however, a difficult one giving that risk in the contemporary techno-scientific era is a realistic proposition. The world risk society has it that risk is ‘system’ immanent and it is inescapable (Beck, 1992).

6.5. Chapter Summary

This chapter has presented detailed analysis and discussion on the determinants of fear of credit/debit card fraud victimisation among university students. The key themes examined included knowledge of cybercrimes, socio-demographic backgrounds, internet use behaviours and prior victimisation experiences. The findings reveal that only internet use behaviour and prior victimisation were significant determinants of fear of credit/debit card fraud. Knowledge of cybercrimes and respondents’ socio-demographic backgrounds were not significantly related to fear of credit/debit card fraud. The fact credit/debit card fraud lacks physicality (visibility) means even though people may have knowledge of cybercrime, they may not be able to relate to its reality. This is especially plausible if such persons have not had first-hand experience of victimisation. Nonetheless, we can infer that respondents are not merely knowledgeable about cybercrime issues but they also employ an element of reflexivity to evaluate the actual prevalence against perceived prevalence of credit/debit card fraud. Reflexivity in this way underscores an important element of the risk society.

The non-significance of socio-demographic backgrounds in relation to fear of cybercrimes is actually intuitive because credit/debit card fraud essentially is characterised by the fact that it is unaffected by physical constraints. Cyberspace is distinguished by “the absence of fixed, empirical constraints and a diffuse, fluid, evolving environment” (Brenner, 2002:39), which goes to justify the non-significance of socio-demographic background in determining people’s fear of credit/debit card fraud victimisation. For example, risk is experienced as gender blind, the reason gender has been found to be non-insignificant. The

same principle applies to all the other socio-demographic demographic variables, and hence, their overwhelming non-significance.

In addition, internet use behaviours significantly increase people's risk of credit/debit card fraud victimisation. This is because frequent internet use exposes users' critical information, such as identification and banking information. These risks remain prevalent, even in the face of user reflexivity (evidenced in personal online precautionary measures), because of the system immanence of risk in the contemporary era (Beck, 1992). Beck's position is in sync with the current study, as the results reveal that students continue to feel at risk, even after utilising various internet use precautionary measures. Even though these measures do not do away with the inherent risks, it thus prevents or reduces actual victimisation.

Finally, the significance of victimisation experience was underscored by the fact people (victims) tend to associate more with what they have already experienced. Negative experiences of the nature gets registered into people's minds and easily come to the fore anytime they come closer to the internet, following their initial victimisation. This perspective is also founded on the constant state of flux which characterises cyberspace. Consequently, the lack of visibility poses a challenge for victims, even after they subsequently employ necessary safeguards. Importantly, some victims of credit/debit card fraud only realise their victimisation several days to weeks after the fact. For such people, victimisation is confirmed only after receiving or accessing their bank statements. Realising victimisation in this way, have long term effects on people and leave them in a constant state of fear. As a result, the inherently risky modern technological era have a disproportionately stronger effect on persons with victimisation experience.

Overall, the importance of internet use behaviours and prior victimisation experiences in explaining fear of credit/debit card fraud suggests that risk is 'system' immanent. This

does not mean that sociodemographic factors and knowledge of crimes are to be ignored but that their contribution to fear might be more related to conventional crimes.

CHAPTER 7

CONCLUSION

This final section presents a synopsis of the main thrusts of the study. The study employed an online survey of students in the University of Saskatchewan over a period of two months. As an explorative study, the research was aimed at identifying the determinants of fear of cybercrime (credit/debit card fraud) victimisation among students.

To facilitate an understanding of the problem under study, the theoretical framework of World Risk Society by Beck was utilised. Essentially in this theory, Beck argues that given the various unintended consequences of the numerous techno-scientific innovations, risks and hazards have become a permanent feature of the modern era (Beck, 1992). Questions were asked across several key variables, which the literature identified as important in predicting peoples' fear of criminal victimisations. Among these variables included knowledge of cybercrime, socio-demographic variables, experience of victimisation and internet use behaviours. Broadly speaking, the study found that victimisation experience and internet use behaviours are both positively associated with students' fear and their risk of becoming victims of credit/debit card fraud.

In particular, the study provides the following answers to my hypotheses:

The study found that socio-demographic factors do not significantly predict fear of credit/debit card fraud victimisation. That is to say, students' socio-demographic identification was unrelated to their fear of credit/debit card fraud victimisation. Specifically, female students have no more significant fear of credit/debit card fraud victimisation than male students; older students have no more significant fear of credit/debit card fraud victimisation than younger students; and single students have no more significant fear of credit/debit card fraud victimisation than non-single students. Additionally, the study again found that students who identify as non-white/non-Caucasian have no more significant fear of

credit/debit card fraud victimisation than students who identify as white/Caucasian; and students in the higher income category, have no more significant fear of credit/debit card fraud victimisation than students in the lower income category.

Also, the study established that knowledge of cybercrime does not significantly influence students' fear of credit/debit card fraud victimisation. That is to say, whether students possess knowledge about cybercrime, or not, makes no significant difference to their fear of credit/debit card fraud victimisation. Specifically, students who hold the view that cybercrime is both cyber-enabled and cyber-dependent have no more significant fear than students who hold the view that cybercrime is either cyber-enabled or cyber-dependent.

Furthermore, the study also revealed that most (a majority) of the internet use behaviours significantly affect students' risk of credit/debit card fraud victimisation. That is to say, a predominant majority of the internet use behaviours significantly increased students' risk of becoming victims of credit/debit card fraud. Specifically, frequent internet use significantly increases students' risk of credit/debit card fraud victimisation; more time spent on the internet (duration) increases students risk of credit/debit card fraud victimisation; and online purchasing activity, as well as frequent online purchasing both increases students' risk of credit/debit card fraud victimisation. Additionally, medium of internet access overwhelmingly affect students' risk of credit/debit card fraud victimisation; and online safety precautions positively affect students' risk of credit/debit card fraud victimisation. However, the study also revealed that place of internet access does not significantly affect students' risk of credit/debit card fraud victimisation.

Finally, the study demonstrates that experience of victimisation significantly affects students' fear of credit/debit card fraud victimisation. More specifically, students with prior experience of victimisation tend to express significantly more fear of becoming victims of credit/debit card fraud.

7.1. Theoretical and Policy implications:

The present study has important implications for theory and policy.

In the realm of theory, the study has established that the theory of risk society is an important and effective framework to help in explaining and predicting fear of credit/debit card fraud victimisation. In other words, the theory has explanatory power as revealed by the study. Risk society theory espouses that risk is 'system' immanent and inescapable, which means that it affects everyone regardless of socio-demographic background such as gender and marital status. This explains why these factors were found to make no significant difference on fear of credit/debit card fraud victimisation. Processes of technological development have led to heightened risks which are experienced as unintended consequences. The risks so experienced, are so prevalent to the extent they become inescapable. This explains the predictive significance of the internet use variables as revealed in the findings.

As well as this, the fact that cybercrime (credit/debit card fraud) takes place in cyberspace, devoid of the physical meeting of victim and offender, means this type of crime is 'blind' to physical space. This implies the commission of such crime is without recourse to the physical and other value or lifestyle identifications of people. Yet again this was confirmed by the predictive non-significance of the socio-demographic variables in the binary logistic regression model. Furthermore the theory also points to the understanding that predictors of fear of criminal victimisations are different depending on the type and context of the crime. This was ascertained from the predictive insignificance of socio-demographic variables in this study contrary to their overwhelming significance in predicting fear of 'conventional' crimes. These finding imply the theory of risk society was very successful in helping our understanding of the problem. For example, the results from all four hypotheses could be explained by the theory, in particular the idea that risk is 'system' immanent and inescapable.

Risk is generally conceived as the outcome of instrumental rationality, and as mainly occurring in the physical world (Fox, 1999). However, drawing on Beck's theory of risk society, I present risk as inescapable, 'system' immanent and ubiquitous. Fear of cybercrimes such as credit/debit card fraud victimisation is an exciting area of focus for researchers because it allows us to draw conclusions about the nature of risks using empirical analyses of a technologically driven phenomenon. By studying determinants of fear of credit/debit card fraud victimisation, we can understand how risk is experienced/manifested in today's technologically driven society. As noted earlier, even though knowledge of cybercrimes and socio-demographic backgrounds were found to be non-significant predictors of fear of credit/card fraud, they offer critical information on how we understand risk. Research on conventional (physical place-based) crimes reveal that knowledge is a significant determinant, but in the context of credit/card fear, it was found non-significant among the university students studied in this research. This means that risk and fear are different in physical and non-physical contexts. Similarly, the non-significance of socio-demographic background in determining fear reveals that risks and fears are no longer place-bound. Instead, it supports Beck's conception that risk is ubiquitous and not limited to particular places. Furthermore, the significance of internet use behaviours and prior experiences of victimisations demonstrate that risks continue to be present.

In addition, I argue that the internet use behaviours and prior victimisation experiences reveal that risks and fears are not becoming obsolete. Instead, they are merely changing forms. The prevalence of internet use presents new avenues of risks and new sources of fears. At the same time, I find that there is continuity with past sources/forms of risks and fear. Prior victimisation experiences are also significant predictors of fears of cybercrimes (credit/debit card fraud), not just conventional physical-based crimes. Thus, rather than rejecting particular conceptualisations of risk, we must see risk as fluid and

changing as context changes (physical to non-physical world). Thus, the study adds support to Beck's risk theory, wherein he conceived risk as system immanent and inescapable. However, it reveals that not all risks are experienced in this way. Risk changes, and for respondents in this study, risks and fear of cybercrimes amplify with frequency of internet use behaviours and prior experiences of victimisations. At the same time, risks and fear of cybercrimes (credit/debit card fraud) are not impacted by socio-demographic backgrounds or knowledge about these crimes. Thus while system immanent, experiences of risks and fears vary depending on contexts.

Policy wise, this study is significant as it enables us to identity the linkages between fear of crimes in the conventional sense and in relation to cybercrime. Like the fear of physical crimes, this study suggests that the fear of cyber-crimes is also partly motivated by perception. In addition, environmental factors also affect the fear of both types of crimes. To this extent, policy makers will have to take necessary steps to reduce negative environmental cues and perceptions. This might include recommending or mandating cyber businesses to provide more visible assurances of their security protocols. In addition, policy makers need to provide more reliable data on the extent of cybercrimes so that people can better manage their perceptions and fears. Steps at increasing reported cases of victimisation should also be pursued, which might require the provision of more safe spaces for victims to do so. By identifying these linkages, policy makers are better positioned to come up with proactive measures to reduce the growing threat of credit/debit card fraud victimisation. For example, knowing that the perpetration of cybercrimes is without recourse to the physical meeting of offender and victim, spatially blind policies and interventions should be targeted to reduce the prevalent risks. Also as the data reveal, frequent internet use significantly increases the risk profile of credit/debit card fraud. Therefore by identifying risk factors, preventative measures can be proposed to eliminate the risks in advance of an explosion of these types of crimes.

Some suggested interventions for policy makers and the relevant stakeholders include educating people on the dangers of online transactions and forming alliances with internet service providers to enhance security. Policy makers can also mandate improved security for online transactions through appropriate legislations. The study is also significant for policy because it addresses a potential future problem, which is an advance in how researchers approach problems. Rather than being reactionary, the results point to the adoption of proactive measures to address fear and risk factors of cybercrimes, especially credit/debit card fraud.

7.3. Limitations and Agenda for future research:

Like all research endeavours, this study was not without its own set of limitations. The fact the study adopted a non-probability sample could pose potential challenges. Significantly, using a non-probability sample means generalisations must be made with caution. It also means we are unable to estimate the sampling error with certainty. However, it is important to add here that I was unable to use a more sophisticated sampling technique because of time constraints and funding challenge as an international graduate student.

Another limitation which is partly related to sampling is the challenge with response rate reporting. This hasn't been included first because the survey was not sent to a panel of respondents. Secondly as a result, the researcher had no idea how many people saw the advertisement but chose not to respond. This is despite the fact the survey was advertised and re-advertised on PAWS (the university's intranet, which is available to all students). However, due to the exploratory nature of the study, the absence of the response rate does not affect the validity of the findings.

Then again another potential limitation of the study is that the study was based on a student population at only a single university. This means we cannot make inferences to the general population.

Additionally, most of the work of theorists on risk seems to contain in them an inherent absence of the trade-off between dangers and benefits of new stuff. The fact that individuals are able, and do tend to take advantage of the benefits of new stuff, hasn't received much credence.

On the way forward, it is recommended that researchers adopt a more holistic approach towards the problem of the fear of cybercriminal victimisation. The research problem should be broadened to include people's motivation for using the internet despite its high risk profile. By so doing, we would better be able to understand the interplay of reflexivity as the key mediating factor from the threshold of risk to victimisation, as Beck's theory argues. In line with the broadened approach, a more sophisticated methodology comprising of a triangulation of methods should be adopted. A quantitative method involving probability sampling should be used together with qualitative interview to enhance representativeness, reliability and validity.

In terms of the coverage or target population, it is recommended that a more general audience should be targeted instead of just limiting to students in the University of Saskatchewan. This will ensure that the outcome of such a study can be more generalisable without much trouble. I would also recommend that the study be pursued from more interdisciplinary and collaborative perspectives to ensure that we develop more nuanced understandings of the problem. In terms of the theoretical approach for future studies, an integrated or synthesised framework comprising of risk theory and James Coleman's rational choice theory is recommended. This will provide an explanation of individuals' motivations for their internet behaviours.

Overall, this study has made significant advances in our understanding of fear of credit/debit card fraud victimisation. Nonetheless, it is important that we continue to extend

our lenses to fully probe prior victimisation experiences and internet use behaviours, and their impact on future fear and their risk that people might feel.

BIBLIOGRAPHY

- Abotchie, C. (1997). *Social control in traditional southern Eweland of Ghana: Relevance for crime prevention*. Accra: Ghana Universities Press.
- Agresti, A. (1990). *Categorical data analysis* New York: Wiley.
- Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey* (Ph.D.). Available from ProQuest Dissertations & Theses Global. (305312893).
- Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, 25(2), 160-171.
- Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer Berlin Heidelberg.
- Arango, C., Huynh, K. P., Fung, B., & Stuber, G. (2012). The changing landscape for retail payments in Canada and the Implications for the demand for cash. *Bank of Canada Review*, 2012 (Autumn), 31-40.
- Arnold, H. (1991). Fear of crime and its relationship to directly and indirectly experienced victimisation: A binational comparison of models. In K. Sessar, & H. Kerner (Eds.), *Developments in crime and crime control research: German studies on victims, offenders, and the public* (pp. 87-125). New York: Springer-Verlag.
- Australian Bureau of Statistics. (2008). *Personal fraud 2007*. Canberra: Author.
- Baumer, T. L. (1978). Research on fear of crime in the United States. *Victimology*, 3(3-4), 254-264.
- Beaulieu, M., Dubé, M., Bergeron, C., & Cousineau, M. (2007). Are elderly men worried about crime? *Journal of Aging Studies*, 21(4), 336-346.
doi:10.1016/j.jaging.2007.05.001
- Beck, U. (1992). *Risk society: Towards a new modernity* (R. Mark Trans.). London: Sage Publications.

- Beck, U. (1996). World risk society as cosmopolitan society?: Ecological questions in a framework of manufactured uncertainties. *Theory, Culture & Society*, 13(4), 1-34. doi:10.1177/0263276496013004001
- Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa - cybercrime and criminality in Ghana. *II* (2), 85-100.
- Box, S., Hale, C., & Andrews, G. (1988). Explaining fear of crime. (Includes bibliography) (Great Britain). *British Journal of Criminology*, 28(3), 340-356.
- Braungart, M. M., Braungart, R. G., & Hoyer, W. J. (1980). Age, sex, and social factors in fear of crime. *Sociological Focus*, 13(1), 55-66.
- Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology*, 4(1), April 5, 2016.
- Bryman, A., Bell, E., & Teevan, J. J. (2012). *Social research methods: Third Canadian edition*. Canada: Oxford University Press.
- Callanan, V., & Rosenberger, J. S. (2015). Media, Gender, and Fear of crime. *Criminal Justice Review*, 40(3), 322-339.
- Canadian Centre for Justice Statistics, & Kowalski, M. (2002). *Cyber-crime [electronic resource]: Issues, data sources, and feasibility of collecting police-reported statistics* Canadian Centre for Justice Statistics.
- Carcach, C., Frampton, P., Thomas, K., & Cranich, M. (1995). Explaining fear of crime in Queensland. *Journal of Quantitative Criminology*, 11(3), 271-287.
- Chiricos, T., Eschholz, S., & Gertz, M. (1997). Crime, news and fear of crime: Toward an identification of audience effects. *Social Problems*, 44(3), 342-357.
- CloudMask. (2016). *The Cost of Data Security: Are cybersecurity investments worth it?* Ottawa: CloudmaskInc. Retrieved from: https://cloudmask.com/data_protection_under_breach/the-cost-of-data-security-are-cybersecurity-investments-worth-it/

- Cox, R. W., Johnson, T. A., & Richards, G. E. (2009). Routine activity theory and internet crime. In Schmallegger, F. and Pittaro, M. (Ed.), *Crimes of the internet* (pp. 302 - 316). New Jersey: Upper Saddle River.
- Creative Research Systems, (2012). Sample size calculator. Retrieved from <http://www.surveysystem.com/sscalc.htm>
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd Ed.). Thousand Oaks, Calif.: Thousand Oaks, Calif.: Sage Publications.
- Croall, H. (2001b). The victims of white-collar crime. In S. Lindgren (Ed.), *White-collar crime research. old views and future potentials: Lectures and papers from a Scandinavian seminar. BRÅ-report 2001:1* (pp. 35-54). Sweden: National Council for Crime Prevention.
- Croall, H. (2009). White collar crime, consumers and victimization. *Crime, Law and Social Change*, 51(1), 127-146.
- Dean, M. (1998)., calculable and incalculable. *Soziale Welt*, 49(1), 25-42.
- Ditton, J., & Farrall, S. (2007). The British crime survey and fear of crime. In M. Hough, & M. Maxfield (Eds.), *Surveying crime in the 21st century* (pp. 223-243). Monsey, NY: Criminal Justice Press.
- Durkin, K. F., & Brinkman, R. (2009). 419 FRAUD: A crime without borders in A postmodern world. *International Review of Modern Sociology*, 35(2), 271-283.
- Elliott, A. (2002). Beck's sociology of risk: A critical assessment. *Sociology*, 36(2), 293-315.
- Farrall, S. (2004). Revisiting crime surveys: Emotional responses without emotions? OR look back at anger. *International Journal of Social Research Methodology*, 7(2), 157-171. doi:10.1080/1304557021000024767
- Farrall, S., Bannister, J., Ditton, J., & Gilchrist, E. (1997). Questioning the Measurement of the 'fear of crime': Findings from a major methodological study. *British Journal of Criminology*, 37(4), 658-679.

- Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. Albany: State University of New York Press.
- Ferraro, K. F. (1996). Women's fear of victimization: Shadow of sexual assault? *Social Forces*, 75(2), 667-690. doi:10.1093/sf/75.2.667
- Fetchenhauer, D., & Buunk, B. P. (2005). How to explain gender differences in fear of crime: Towards an evolutionary approach. *Sexualities, Evolution & Gender*, 7(2), 95-113. doi:10.1080/00207170500111044
- Fox, N. (1999). Postmodern reflections on 'risk', 'hazards' and life choices. In D. Lupton (Ed.), *Risk and sociocultural theory: New directions and perspectives* (pp. 12-33). Cambridge: Cambridge University Press.
- Fox, S., & Lewis, O. (2001). Fear of online crime. *Pew Internet Tracking Report*,
- Franklin, C. A., & Franklin, T. W. (2009). Predicting fear of crime: Considering differences across gender. *Feminist Criminology*, 4(1), 83-106. doi:10.1177/1557085108325196
- Friedman, K., Bischoff, H., Davis, R., & Person, A. (1982). *Victims and helpers: Reactions to crime*. New York: US Department of Justice, National Institute of Justice.
- Garofalo, J. (1981). The fear of crime: Causes and consequences. (Symposium on victimization and victimology). *Journal of Criminal Law and Criminology*, 72(2), 839-857.
- Gerbner, G., Gross, L., Morgan, M., & Signorielli, N. (1980). The "mainstreaming" of America: Violence profile no. 11. *Journal of Communication*, 30(3), 10-29. doi:10.1111/j.1460-2466.1980.tb01987.x
- Giddens, A. (1976). *New Rules of Sociological Method*. New York: Basic Books.
- Giddens, A. (1998a). Risk society: The context of British politics. In J. Franklin (Ed.), *The politics of risk society* (pp. 23-34). Cambridge: Polity Press.
- Giddens, A. (1999). *Runaway world: How globalisation is reshaping our lives* Profile books.

- Giddens, A. (1994). *Beyond left and right: The future of radical politics*. Stanford, Calif.: Stanford, Calif. : Stanford University Press.
- Grabosky, P. (2001). Virtual criminality: Old wine in new bottles?(the nature of virtual criminality). *Social & Legal Studies*, 10(2), 243-249.
- Grau, J. (2008). *CanadaB2C E-Commerce: A Work in Progress*. New York: eMarketer.
- Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology*, 4(2), 79-150.
- Healey, J. F. (2009). *Statistics: A tool for social research* (Eighth ed.) Belmont CA: Wadsworth Cengage Learning.
- Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, 1043986213507403. doi:10.1177/1043986213507403
- Hird, M. J. (2012). *Sociology of science: A critical Canadian introduction*. Toronto: Oxford University Press.
- Holtfreter, K., Reisig, M. D., Leeper Piquero, N., & Piquero, A. R. (2010). Low self- control and fraud: Offending, victimization, and their overlap. *Criminal Justice and Behavior*, 37(2), 188-203. doi:10.1177/0093854809354977
- Jackson, J. (2004). Experience and expression: Social and cultural significance in the fear of crime.(author abstract). *British Journal of Criminology*, 44(6), 946.
- Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. *Crimes of the Internet*, , 283-301.
- Keane, C. (1992). Fear of crime in Canada: An examination of concrete and formless fear of victimization. *Canadian Journal of Criminology*, 34(2), 215-224.
- Killias, M. (1990). Vulnerability: Towards a better understanding of a key variable in the genesis of fear of crime. *Violence and Victims*, 5(2), 97.

- Kowalski, M., Statistics Canada, & Canadian Centre for Justice Statistics. (2002). *Cyber-crime*. Ottawa: Statistics Canada.
- Lane, J., & Fisher, B. S. (2009). Unpacking the relationship between gender and fear of crime: Explaining why there are similarities and differences. *Journal of Contemporary Criminal Justice*,
- Lastowka, F. G., & Hunter, D. (2004). Virtual Crimes. *New York Law School Review*, 49, 293-316.
- Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & and Isabalija, R. (2009). Seeing beyond the surface: Understanding and tracking fraudulent cyber activities. *International Journal of Computer Science and Information Security*, 6(3), 124 - 135.
- Maat, S. M. (2009). *Cyber crime: A comparative law analysis*. (Unpublished LLM). University of South Africa, Pretoria,
- Maguire, M., & Corbett, C. (1987). *The effects of crime and the work of victims support schemes* Cambridge Studies in Criminology LVI, Gower Aldershot.
- Mann, D., & Sutton, M. (1998). " Netcrime: More change in the organization of thieving. *British Journal of Criminology, Delinquency and Deviant Social Behaviour*, 38, 201-29.
- Mawby, R., & Walklate, S. (1994). *Critical victimology: The victim in international perspective* London: Sage.
- Mawby, R. I., & Gill, M. L. (1987). *Crime victims: Needs, services, and the voluntary sector* (Volume 377 ed.) Taylor & Francis.
- Mazowita, B., & Vézina, M. (2014). Police-reported cybercrime in Canada, 2012. *Juristat: Canadian Centre for Justice Statistics*, , 1-24.
- McCullagh, P., & Nelder, J. A. (1989). *Generalized linear models* CRC press.
- McCusker, R. (2006). Transnational Organised cyber crime: Distinguishing threat from reality. *Crime, Law and Social Change*, 46(4-5), 257-273.

- McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of Key Findings and Implications. Home Office Research Report, 75*
- Merry, S. E. (1981). *Urban danger: Life in a neighborhood of strangers* Temple University Press: Philadelphia.
- Mesch, G. S. (2000). Women's fear of crime: The role of fear for the well- being of significant others. (Statistical data included). *Violence and Victims, 15*(3), 323-336.
- Mesko, G., & Bernik, I. (2011). Cybercrime: Awareness and fear: Slovenian perspectives. *Intelligence and Security Informatics Conference (EISIC), 2011 European, 28-33.*
- Ministry of Public Safety. (2009). *Public Safety and Emergency Preparedness Canada: 2009-10 Report on Plans and Priorities*, Ministry of Public Safety, Ottawa. Retrieved from Ministry of Public Safety website: <http://www.tbs-sct.gc.ca/rpp/2009-2010/inst/psp/psp-eng.pdf>
- Nukunya, G. K. (2003). *Tradition and change in ghana: An introduction to sociology*. Accra: Ghana Universities Press.
- Ortega, S. T., & Myles, J. L. (1987). Race and gender effects on fear of crime: An interactive model with age*. *Criminology, 25*(1), 133-152. doi:10.1111/j.1745-9125.1987.tb00792.x
- Oxford Dictionaries: Language Matters. (2014). Cybercrime. Retrieved from <http://www.oxforddictionaries.com/definition/english/cybercrime>
- Parker, K. D. (1988). Black-white differences in perceptions of fear of crime. *The Journal of Social Psychology, 128*(4), 487-494.
- Parker, K. D., & Ray, M. C. (1990). Fear of crime: An assessment of related factors. *Sociological Spectrum, 10*(1), 29-40. doi:10.1080/02732173.1990.9981910
- Parker, K., McMorris, B., Smith, E., & Murty, K. (1993). Fear of crime and the likelihood of victimization: A bi- ethnic comparison. *Journal of Social Psychology, 133*(5), 723.

- Parliamentary Joint Committee on the Australian Crime Commission (PJCACC). (2004). Supplementary report to the inquiry into the trafficking of women for sexual servitude. *Canberra: Parliament of the Commonwealth of Australia*,
- Payne, B. K., & Chappell, A. (2008). Using student samples in criminological research. *Journal of Criminal Justice Education*, 19(2), 175-192.
doi:10.1080/10511250802137226
- Prensky, M. (2001). Digital natives, digital immigrants part 2: Do they really think differently? *On the Horizon*, 9(6), 1-6. doi:10.1108/10748120110424843
- Rasborg, K. (2012). '(World) risk society' or 'new rationalities of risk'? A critical discussion of Ulrich Beck's theory of reflexive modernity. *Thesis Eleven*, 108(1), 3-25.
- Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, 20(3), 315-328.
- Schafer, J. A., Huebner, B. M., & Bynum, T. S. (2006). Fear of crime and criminal victimization: Gender-based contrasts. *Journal of Criminal Justice*, 34(3), 285-301.
doi:10.1016/j.jcrimjus.2006.03.003
- Shapiro, S. P. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime. *American Sociological Review*, 55(3), 346-365.
- Shrum, L. J., & Bischak, V. D. (2001). Mainstreaming, resonance, and impersonal impact testing moderators of the cultivation effect for estimates of crime risk. *Human Communication Research*, 27(2), 187.
- Skogan, W. G. (1990). *Disorder and decline: Crime and the spiral of decay in American cities*. New York, NY: The Free Press.
- Skogan, W. G. (1993). The various meanings of fear. In W. Bilsky, C. Pfeiffer & P. Wetzels (Eds.), *Fear of crime and criminal victimization* (pp. 131-141). Stuttgart, Germany: Enke.
- Skogan, W. G. (1987). The impact of victimization on fear. *Crime & Delinquency*, 33(1), 135-154.

- Slapper, G., & Tombs, S. (1999). In Tombs S. (Ed.), *Corporate crime*. Harlow: Harlow: Longman.
- Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, 58(1), 22-23. doi:10.1080/09627250408553240
- Smith, W. R., & Torstensson, M. (1997). Gender differences in Risk Perception and neutralizing Fear of Crime: Toward resolving the paradoxes.37 (4), 608-634.
- Smyth, S. M. (2010). *Cybercrime in Canadian criminal law*. Toronto: Toronto: Carswell.
- StatsCan. (2009). *Internet shopping in Canada: An examination of data, trends and patterns* (Publication no. [88F0006X](#)). Retrieved from Statistics Canada website: <http://www.statcan.gc.ca/pub/88f0006x/2009005/part-partie1-eng.htm>
- Taylor, R. B., & Hale, M. (1986). Testing alternative models of fear of crime. *The Journal of Criminal Law and Criminology (1973-)*, 77(1), 151-189. doi:10.2307/1143593
- Tombs, S. (1999). Health and safety crimes :(in) visibility and the problems of 'Knowing'. In P. Davies, P. Francis & V. Jupp (Eds.), *Invisible crimes: Their victims and their regulation* (pp. 77-104). New York: St Martins Press.
- University of Saskatchewan. (2015). Student headcount and demographics, information & communications technology – reporting and data services. Retrieved from <http://www.usask.ca/isa/statistics/students/headcount-demographics.php>
- Valiquet, D. (2011). *Cybercrime: Issues* (Publication No. 2011-36-E). Library of Parliament, Ottawa, Canada. Retrieved from Library of Parliament website: <http://www.lop.parl.gc.ca/content/lop/researchpublications/2011-36-e.pdf>
- Wall, D. S. (1999). Cybercrimes: New wine, no bottles? In P. Davies, P. Francis & V. Jupp (Eds.), *Invisible crimes: Their victims and their regulation* (pp. 105-39). London: Macmillan.
- Wall, D. S. (2001). Cybercrimes and the internet. In D. Wall (Ed.), *Crime and the internet* (). London: Routledge.

- Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, 5(1), 736 - 749.
- Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. *Criminal Justice*, 4(4), 451-489.
- Weinrath, M., Clarke, K., & Forde, D. R. (2007). Trends in fear of crime in a western Canadian city: 1984, 1994, and 2004. *Canadian Journal of Criminology and Criminal Justice*, 49(5), 617-646. doi:doi:10.3138/cjccj.49.5.617
- Whitrod, R. (1982). Problems in the measurement of the fear of crime. *Victims of Crime Service, Adelaide*,
- Yang, S., & Wyckoff, L. A. (2010). Perceptions of safety and victimization: Does survey construction affect perceptions? *Journal of Experimental Criminology*, 6, 293-323. doi:10.1007/s11292-010-9100-x
- Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407-427. doi: 10.1177/147737080556056
- Yin, P. P. (1980). Fear of crime among the elderly: Some issues and suggestions. *Social Problems*, 27(4), 492-504. doi:10.2307/800177
- Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, 8(1), 36-46.

APPENDIX

Survey Questionnaire

Consent Statement: This survey is designed to contribute towards understanding the determinants of cybercrime victimisation among students, with a focus on credit/debit card fraud. The objective is to understand the incidence of the fear of cybercrime victimisation among students, and to situate the phenomenon theoretically within a sociological lens. Participation in this survey is voluntary, and you can decide not to participate at any time, or choose not to answer any questions you don't feel comfortable with. Survey responses will remain anonymous. Since the survey is anonymous, once it is submitted it cannot be removed. There are no known risks to participating in this survey; however, as with any online related activity the risk of breach of confidentiality is always possible. This survey is hosted by Qualtrics, a company located in the USA and subject to US laws and whose servers are located outside of Canada. The privacy of the information you provide is subject to the laws of those other jurisdictions. By participating in this survey you acknowledge and agree that your [answers/information] will be stored outside of Canada and may or may not receive the same level of privacy protection. The privacy policy for the web survey company can be found at the following link: <http://www.qualtrics.com/privacy-statement>. Completion of the survey should take between 10 to 15 minutes. This research project has been approved on ethical grounds by the University of Saskatchewan Research Ethics Board. Any questions regarding your rights as a participant may be addressed to that committee through the Research Ethics Office ethics.office@usask.ca (306) 966-2975. By completing and submitting this questionnaire, your free and informed consent is implied and indicates that you understand the above conditions of participation in this study.

Q1. In your view, what constitutes cybercrime?

- ☐ Crimes committed using computer or its systems as the tool (cyber-enabled) (1)
- ☐ Crimes committed using computer or its systems as the target (cyber-dependent) (2)
- ☐ All of the above (3)

Q2. In your view, over the last couple of years do you think cybercrime has ...

- ☐ Increased substantially (1)
- ☐ Increased somewhat (2)
- ☐ Remained the same (3)
- ☐ Decreased somewhat (4)
- ☐ Decreased substantially (5)

Q3. Have you had experience with physical crimes (e.g. physical assault, burglary etc) in the past 12 months?

- ☐ Yes (1)
- ☐ No (2)

Q4. Compared to other crimes (physical crimes), do you feel more at risk of Credit/Debit Card fraud?

- ☐ Yes (1)
- ☐ No (2)

Q5. How did you first come to learn about Credit/Debit card fraud?

- ☐ The news media (1)
- ☐ Social media (2)
- ☐ Friends (3)
- ☐ Personal experience (4)

- ☐ Personal research (5)
- ☐ Other (specify) ... (6) _____

Q6. During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?

- ☐ Yes (1)
- ☐ No (2)

Answer If During the past month, have you ever felt fearful about being the victim of credit/debit card fraud? Yes Is Selected

Q7. How many times have you felt like this in the past month? Record number times ...

Answer If During the past month, have you ever felt fearful about being the victim of credit/debit card fraud? Yes Is Selected

Q8. Consider a time in the past month you felt MOST fearful about being the victim of credit card fraud. On a scale of 0 to 5, where 0=not at all fearful and 5=extremely fearful, how fearful were you?

- ☐ 0 (Not at all fearful) (1)
- ☐ 1 (2)
- ☐ 2 (3)
- ☐ 3 (4)
- ☐ 4 (5)
- ☐ 5 (Extremely fearful) (6)

Q9. During the past 12 months, did anyone steal your credit/debit card or use your card information, without your permission to obtain money or credit?

- ☐ Yes (1)
- ☐ No (2)

Answer If During the past 12 months did anyone steal your credit/debit card or use your card information without your permission to obtain money or credit? Yes Is Selected

Q10. How many times did that happen to you? Record number: ...

- ☐ 1 time (1)
- ☐ 2 times (2)
- ☐ 3 times (3)
- ☐ 4 times (4)
- ☐ 5 or more times (5)

Answer If During the past 12 months did anyone steal your credit/debit card or use your card information without your permission to obtain money or credit? Yes Is Selected

Q11. Where was your credit/debit card information stolen (choose all that apply?)

- ☐ On my cell phone (1)
- ☐ Tablet (2)
- ☐ Laptop (3)
- ☐ Desktop (4)

Answer If During the past 12 months, did anyone steal your credit/debit card or use your card information, without your permission to obtain money or credit? Yes Is Selected

Q12. Would you consider one or more of your experience with the theft of your credit/debit card information to be a cybercrime?

- ☐ Yes (1)
- ☐ No (2)
- ☐ In some cases (3)

Q13. Where do you mostly access internet from?

- ☐ Home (1)
- ☐ School (2)
- ☐ Public computer (library, cyber cafe) (3)
- ☐ Other (please specify) ... (4) _____

Q14. How do you access the internet? (please select all that apply)

- ☐ On my phone (1)
- ☐ Tablet (2)
- ☐ Laptop (3)
- ☐ Desktop (4)
- ☐ Other (please specify) ... (5) _____

Q15. How frequently do you use the internet?

- ☐ Once daily (1)
- ☐ Several times in a day (2)
- ☐ Weekly (3)
- ☐ Monthly (4)

Q16. On average, how much time do you spend on the internet each time you go online?

- ☐ Less than 30 minutes (1)
- ☐ Over 30 minutes but less than an hour (2)
- ☐ Between 1 and 2 hours (3)
- ☐ Over 2 hours (4)

Q17. During the past 12 months, have you used the internet to purchase anything online?

☐ Yes (1)

☐ No (2)

Answer If During the past 12 months have you used the internet to purchase anything online? Yes Is Selected

Q18. About how many times a month did you purchase something online, during the past year?

☐ 1-5 times (1)

☐ 6-10 times (2)

☐ 11-15 times (3)

☐ More than 15 times (4)

Q19. What specific safety precautions do you employ while using the internet – to shop online or to access sensitive information?(choose all that apply)

☐ I always shop on safe sites (1)

☐ I always ensure I have an updated anti-virus on my system (2)

☐ I don't use public computers for online banking or shopping transactions (3)

☐ I don't respond to anonymous emails (4)

☐ I don't run unknown applications on my computer (5)

☐ I change my passwords frequently (6)

☐ I check my credit report/banking or credit card statement frequently (7)

☐ Other (please specify) ... (8) _____

☐ I do not employ any safeguards while using the internet (9)

Q20. To your knowledge, does your bank employ security measures to protect customers during their online transactions?

☐ Yes (1)

☐ No (2)

Answer If To your knowledge does your bank employ security measures to protect customers during their online transactions? >Yes Is Selected

Q21. To your knowledge, which security measures does your bank use to safeguard your online transactions?

☐ Security software (1)

☐ Security key (2)

☐ Encryption technology (3)

☐ Automatic logout after 10 minutes of inactivity (4)

☐ Digital certificates with trusted third party companies (5)

☐ Other (please specify) ... (6) _____

Q22. Please indicate your gender?

☐ Male (1)

☐ Female (2)

☐ Other (please specify) ... (3) _____

☐ Prefer not to say (4)

Q23. Please indicate your age range...

☐ Under 17 years (1)

☐ 17-23 years (2)

☐ 24-30 years (3)

☐ 31-37 years (4)

☐ 38-44 years (5)

- ☐ 45-51 years (6)
- ☐ 52 and over (7)

Q24. Please indicate your level of studies...

- ☐ Undergraduate 1st year (1)
- ☐ Undergraduate 2nd year (2)
- ☐ Undergraduate 3rd year (3)
- ☐ Undergraduate 4th year or more (4)
- ☐ Graduate 1st year (5)
- ☐ Graduate 2nd year (6)
- ☐ Graduate 3rd year (7)
- ☐ Graduate 4th year or more (8)
- ☐ Other (please specify) ... (9) _____

Q25. Are you studying full time or part-time?

- ☐ Full time (1)
- ☐ Part time (2)
- ☐ Not applicable (4)

Q26. What is your Residency status?

- ☐ Domestic Student (citizen or permanent resident) (1)
- ☐ International Student (2)

Q27. What ethnicity do you identify with?

- ☐ Aboriginal (1)
- ☐ White/Caucasian (2)
- ☐ African (3)
- ☐ Asian (4)

- ☐ Other (please specify) ... (5) _____

Q28. Please indicate your current marital status?

- ☐ Single (Never legally married) (1)
- ☐ Legally married (and not separated) (2)
- ☐ Separated, but still legally married (3)
- ☐ Living with a common-law partner (4)
- ☐ Divorced (5)
- ☐ Widowed (6)

Q29. What category best describes your annual total family income, from all sources before taxes?

- ☐ Less than \$25,000 (1)
- ☐ \$25,000 to less than \$50,000 (2)
- ☐ \$50,000 to less than \$75,000 (3)
- ☐ \$75,000 to less than \$100,000 (4)
- ☐ \$100,000 to less than \$125,000 (5)
- ☐ \$125,000 or more (6)
- ☐ Don't know/Prefer not to say (7)

Q30. Please indicate your place of residence...

- ☐ University residence (1)
- ☐ Off campus urban (2)
- ☐ Off campus rural (3)

Q31. What best describes your current employment status?

- ☐ Working part time (1)
- ☐ Working full time (2)

○ Not working (3)